SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.	PAGE 1 OF
	32

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NO.	6. SOLICITATION ISSUE DATE
NNH13CH30Z	02/01/2013		NNH12424505Q	

7. FOR SOLICITATION INFORMATION CALL	7a. NAME	7b. TELEPHONE NO.	8. OFFER DUE DATE/LOCAL TIME
	Cedric M.T. Mitchener	(301) 286-6162	

9. ISSUED BY	CODE	10. THIS ACQUISITION IS
NASA Goddard Space Flight Center Office for Headquarters Greenbelt, MD 20771	210.H	☒ UNRESTRICTED OR ☐ SET ASIDE % FOR ☐ SMALL BUSINESS ☐ HUBZONE SMALL BUS. NAICS: 541519 ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS SIZE STANDARD: $25.5M ☐ 8(A) ☐ EMERGING SMALL BUSINESS

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING
☐ SEE SCHEDULE	NET 30 days	☐	N/A

14. METHOD OF SOLICITATION
☒ RFQ ☐ IFB ☐ RFP

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE
As Indicated On Each Call		NASA Goddard Space Flight Center Office for Headquarters Greenbelt, MD 20771	210.H

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
INFOZEN, INC 9420 KEY WEST AVE STE 101 ROCKVILLE MD 20850-6379	1QVG9		See Item 33 - Clause GSFC 52.232-95, "Invoices - Submission of"	NSSC

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOW IN BLOCK 18a UNLESS BLOCK ON RIGHT IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	GSA Contract #: GS-35F-0209V Web Enterprise Service Technologies (WEST) PRIME as described in the Statement of Work (SOW) of this Blanket Purchase Agreement (BPA) under Attachment A.				

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT (Govt. Use Only)
As Indicated on Each Call	$0.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

☐ 29. AWARD OF CONTRACT: REFERENCE _____ OFFER DATED _____ YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (Signature of Contracting Officer)

30b. NAME AND TITLE OF SIGNER (Type or Print)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (Type)	31c. DATE SIGNED
		CEDRIC M.T. MITCHENER	

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

Standard Form 1449 (REV. 3/2005)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN ☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED _____			
32b. SIGNATURE OF AUTHORIZED GOVT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
32e. MAILING ADDRESS OF AUTHORIZED GOVT. REPRESENTATIVE		32f. TELEPHONE NO. OF AUTHORIZED GOVT REPRESENTATIVE 32g. EMAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
33. SHIP NO. ☐ PARTIAL ☐ FINAL	34. VOUCHER NO.	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL
37. CHECK NO.			
38. S/R/ACCOUNT NO.	39. VOUNCHER NO.	40. PAID BY	
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY (Print)	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT (Location)	
		42c. DATE REC'D	42d. TOTAL CONTAINERS

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
GODDARD SPACE FLIGHT CENTER
OFFICE FOR HEADQUARTERS, CODE 210.H
BLANKET PURCHASE AGREEMENT

Pursuant to General Services Administration (GSA) Federal Supply Schedule (FSS) Information Technology (IT) 70 against Contract Number ***GS-35F-0209V*** *and Federal Acquisition Regulation (FAR) 8.405-3, "Blanket Purchase Agreements (BPAs)", the Contractor agrees to the following terms of a BPA exclusively with National Aeronautics and Space Administration (NASA):*

(1) All orders placed against this BPA shall be on a firm fixed price basis and shall be within the scope of the Statement of Work (SOW) under Attachment A of this BPA.

(2) Pricing of task orders placed under this BPA shall be based on the discounted GSA contract pricing identified in the Loaded Labor Rate Matrix under Attachment B of this BPA. Prompt payment discounts are not offered.

(3) All orders placed against this BPA are subject to the terms and conditions of the GSA contract and this BPA. In the event of any inconsistency between the terms and conditions of this BPA and a Task Order issued against it, the BPA shall take precedence. The Contracting Officer shall be contacted in the event there are any issues/disagreements regarding the terms and conditions of this BPA.

(4) This BPA contains clauses and provisions taken from, among other sources, the Federal Acquisition Regulation (FAR) and the NASA FAR Supplement (NFS). Whenever the word "contract" appears in FAR and NFS clauses and provisions presented herein, substitute the word "BPA" respectively. In addition, throughout this entire document, the term "Contracting Officer" refers to the NASA Contracting Officer, Code 210.H, except where specifically defined otherwise.

(5) Delivery destinations and schedules will be indicated on individual orders placed against this BPA.

(6) This BPA does not obligate any funds. In addition, the Government is obligated only to the extent of authorized orders actually made under this BPA.

(7) The Government estimates, but does not guarantee, that the volume of purchases through this BPA(s) will be $40 million.

(8) The ordering period for this BPA is for a one-year base and 4 one-year options from the effective date, or at the end of the GSA Schedule contract period, whichever is earlier.

(9) The following office(s) is hereby authorized to place orders under this BPA:

NASA Goddard Space Flight Center (GSFC)
Office for Headquarter, Code 210.H
Greenbelt, Maryland 20771

NOTE: No changes to this BPA shall be made without proper authorization from the assigned Contracting Officer in Code 210.H.

(End of Text)

(10) CONTRACTING OFFICER'S REPRESENTATIVE (COR)

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

Tracee McCall
NASA/Headquarters
Phone: (202) 358 – 2056
E-Mail: Tracee.M.McCall@nasa.gov

Note: Each individual task order will identify the appropriate task order Technical Lead/Representative.

(End of Text)

(11) INVOICES AND PAYMENT

(a) Invoices shall be submitted after completion of service outlined in each individual task order. The Contractor shall submit invoices as specified under Item 33, "(GSFC 52.232-95) INVOICES – SUBMISSION OF (AUG 2008) for this BPA, with one copy each to the Contracting Officer and the Contracting Officer's Representative (COR).

(b) The invoice must include the name and address of the contractor, invoice date and number, BPA and task order numbers, description of the services/supplies, and include a breakdown of the support by individual by GSA labor category performing the service. Travel and other direct costs (ODC's) shall be broken out separately, in adequate detail, and listed on the invoice as instructed in Task Orders issued against this BPA. Invoices shall be submitted to and approved for payment by the Contracting Officer. Invoices shall contain a statement certifying the actual number of direct labor hours expended. Invoices shall provide labor hour details by SOW activity/task by GSA Labor Category.

(c) Invoices shall be submitted monthly in arrears for actual labor hours, travel expenses, and other direct costs. Fractional parts of an hour shall be payable on a prorated basis. Invoices shall include a breakdown of the skill categories by individual's name and labor hours charged. Travel costs shall be reimbursed in accordance with FAR 31.205-46 and the Federal Travel Regulations. Travel invoices shall be broken down in the invoice by individual, number of days, and shall include airfare (origin/destination), reason for travel, per diem rate, and car rental. Travel receipts may be requested by the Contracting Officer and provided by the Contractor for lodging, car rentals, and any other travel expenditures.

(d) Within 60 days after the expiration of the final task order, the Contractor shall submit one of the following to the Contracting Officer: A final invoice marked "Final" for all outstanding charges or a statement that there are no outstanding charges. The Contracting Officer may at any time before final payment is made under this BPA request an audit of the invoices submitted for payment.

(e) The Government shall not be obligated to pay the Contractor any amount in excess of the ceiling price outlined in each individual task order and shall not exceed the ceiling price outlined in the BPA schedule under the Deliverable Requirements provision, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the task order and BPA schedule. The Contractor is required to notify the Contracting Officer at least 30 days in advance and in writing if it is necessary to revise the ceiling price and provide the reason why the work cannot be performed under the current ceiling price of the task order. The Contracting Officer may determine it is in the best interest of the Government to issue a modification to the task order to increase the ceiling price. The Contractor agrees to perform the work specified in the schedule and all obligations under each individual task order and this BPA within such ceiling price.

(End of Text)

(12) SUPPLIES AND/OR SERVICES TO BE FURNISHED

(a) The Contractor shall provide all resources, services, personnel, and facilities necessary to perform the work as specified in the SOW under Attachment A and the individual task orders. The Direct Labor Rates are in accordance with the Loaded Labor Rate Matrix under Attachment B.

The Contractor shall deliver the following documentations and reports:

Item	Description	Reference	Schedule	Delivery Method/Addressee(s)
1	Services and Deliverables in accordance with the SOW and Task Orders	Attachment A – Statement of Work and individual task orders	As defined in individual task orders	See Task Order(s)
2	IT Security Plan & Management Plan	Item (16) of BPA, NFS 1852.204-76 / Attachment E	30 days after BPA effective date	Electronic Format to the Contract Specialist
3	Task Plans	Item (18) of BPA, NFS1852.216-80	Within 7 calendar days after receipt of request for task plan	Electronic Format to the Contract Specialist
4	Organizational Conflicts of Interest (OCI) Avoidance Plan	Item (20) of BPA, NFS 1852.237-72 / Attachment F	30 days after BPA effective date	Electronic Format to the Contract Specialist

(13) PLACE OF PERFORMANCE

The services specified by this contact shall be performed at the following location(s):

NASA Headquarters, the Contractor's facilities and any other location deemed necessary by the Government.

NASA Locations		Contractor's Facilities
Ames Research Center (ARC)	Johnson Space Center (JSC)	9420 Key West Ave., Suite 101 Rockville, MD 20850-6379
Dryden Flight Research Center (DFRC)	Kennedy Space Center (KSC)	
Glenn Research Center (GRC)	Langley Research Center (LaRC)	
Goddard Institute of Space Studies (GISS)	Marshall Space Flight Center (MSFC)	
Goddard Space Flight Center (GSFC)	NASA Shared Service Center (NSSC)	
Headquarters (HQ)	Stennis Space Center (SSC)	
IV and V Facility	Wallops Flight Facility	
Jet Propulsion Laboratory (JPL)	White Sands Test Facility	

(End of Text)

(14) (FAR 52.252-2) CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address (es):

Federal Acquisition Regulation (FAR) clauses:
https://www.acquisition.gov/far/

NASA FAR Supplement (NFS) clauses:
http://www.hq.nasa.gov/office/procurement/regs/nfstoc.htm

(15) In addition to the GSA contract schedule clauses, this BPA is subject to the following clauses:

NFS 1852.219-76	NASA 8 PERCENT GOAL (JULY 1997)
NFS 1852.223-75	MAJOR BREACH OF SAFETY OR SECURITY (FEB 2002)
NFS 1852.225-70	EXPORT LICENSES (FEB 2000)
NFS 1852.228-75	MINIMUM INSURANCE COVERAGE (OCT 1988)
NFS 1852.243-71	SHARED SAVINGS (MARCH 1997)

(End of Section)

(16) (NFS 1852.204-76) SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JAN 2011)

(a) The contractor shall protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure.

(b) This clause is applicable to all NASA contractors and sub-contractors that process, manage, access, or store unclassified electronic information, to include Sensitive But

Unclassified (SBU) information, for NASA in support of NASA's missions, programs, projects and/or institutional requirements. Applicable requirements, regulations, policies, and guidelines are identified in the Applicable Documents List (ADL) provided as an attachment to the contract. The documents listed in the ADL can be found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. For policy information considered sensitive, the documents will be identified as such in the ADL and made available through the Contracting Officer.

(c) Definitions.

(1) IT resources means any hardware or software or interconnected system or subsystem of equipment, that is used to process, manage, access, or store electronic information.

(2) NASA Electronic Information is any data (as defined in the Rights in Data clause of this contract) or information (including information incidental to contract administration, such as financial, administrative, cost or pricing, or management information) that is processed, managed, accessed or stored on an IT system(s) in the performance of a NASA contract.

(3) IT Security Management Plan--This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. Unlike the IT security plan, which addresses the IT system, the IT Security Management Plan addresses how the contractor will manage personnel and processes associated with IT Security on the instant contract.

(4) IT Security Plan--this is a FISMA requirement; see the ADL for applicable requirements. The IT Security Plan is specific to the IT System and not the contract. Within 30 days after award, the contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer; the approval authority will be included in the ADL. All contractor personnel requiring physical or logical access to NASA IT resources must complete NASA's annual IT Security Awareness training. Refer to the IT Training policy located in the IT Security Web site at https://itsecurity.nasa.gov/policies/index.html.

(d) The contractor shall afford Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA Electronic Information or to the function of IT systems operated on behalf of NASA, and to preserve evidence of computer crime.

(e) At the completion of the contract, the contractor shall return all NASA information and IT resources provided to the contractor during the performance of the contract in accordance with retention documentation available in the ADL. The contractor shall provide a listing of all NASA Electronic information and IT resources generated in performance of the contract. At that time, the contractor shall request disposition instructions from the Contracting Officer. The Contracting Officer will provide disposition instructions within

30 calendar days of the contractor's request. Parts of the clause and referenced ADL may be waived by the contracting officer, if the contractor's ongoing IT security program meets or exceeds the requirements of NASA Procedural Requirements (NPR) 2810.1 in effect at time of award. The current version of NPR 2810.1 is referenced in the ADL. The contractor shall submit a written waiver request to the Contracting Officer within 30 days of award. The waiver request will be reviewed by the Center IT Security Manager. If approved, the Contractor Officer will notify the contractor, by contract modification, which parts of the clause or provisions of the ADL are waived.

(f) The contractor shall insert this clause, including this paragraph in all subcontracts that process, manage, access or store NASA Electronic Information in support of the mission of the Agency.

(End of Clause)

(17) (NFS1852.215-84) OMBUDSMAN (NOV 2011) ALTERNATE (JUNE 2000)

(a) An ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and contractors during the preaward and postaward phases of this acquisition. When requested, the ombudsman will maintain strict confidentiality as to the source of the concern. The existence of the ombudsman is not to diminish the authority of the contracting officer, the Source Evaluation Board, or the selection official. Further, the ombudsman does not participate in the evaluation of proposals, the source selection process, or the adjudication of formal contract disputes. Therefore, before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommendations to the contracting officer for resolution.

(b) If resolution cannot be made by the contracting officer, interested parties may contact the installation ombudsman. The current list of Center Ombudsman is available at http://prod.nais.nasa.gov/pub/pub_library/Omb.html. Concerns, issues, disagreements, and recommendations which cannot be resolved at the installation may be referred to the NASA ombudsman, the Director of the Contract Management Division, at 202-358-0445, facsimile 202-358-3083. Please do not contact the ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries shall be directed to the Contracting Officer or as specified in this document.

(c) If this is a task or delivery order contract, the ombudsman shall review complaints from contractors and ensure they are afforded a fair opportunity to be considered, consistent with the procedures of the contract.

(End of Clause)

(18) (NFS1852.216-80) TASK ORDERING PROCEDURE (OCT 1996)

(a) Only the Contracting Officer may issue task orders to the Contractor, providing specific authorization or direction to perform work within the scope of the contract and as specified in the schedule. The Contractor may incur costs under this contract in

performance of task orders and task order modifications issued in accordance with this clause. No other costs are authorized unless otherwise specified in the contract or expressly authorized by the Contracting Officer.

(b) Prior to issuing a task order, the Contractor Officer shall provide the Contractor with the following data:

(1) A functional description of the work identifying the objectives or results desired from the contemplated task order.
(2) Proposed performance standards to be used as criteria for determining whether the work requirements have been met.
(3) A request for a task plan from the Contractor to include the technical approach, period of performance, appropriate cost information, and any other information required to determine the reasonableness of the Contractor's proposal.

(c) Within seven (7) calendar days after receipt of the Contracting Officer's request, the Contractor shall submit a task plan conforming to the request.

(d) After review and any necessary discussions, the CO may issue a task order to the Contractor containing, as a minimum, the following:

(1) Date of the order.
(2) Contract number and order number.
(3) Functional description of the work identifying the objectives or results desired from the task order, including special instructions or other information necessary for performance of the task.
(4) Performance standards, and where appropriate, quality assurance standards.
(5) Maximum dollar amount authorized (cost and fee or price). This includes allocation of award fee among award fee periods, if applicable.
(6) Any other resources (travel, materials, equipment, facilities, etc.) authorized.
(7) Delivery/performance schedule including start and end dates.
(8) If contract funding is by individual task order, accounting and appropriation data.

(e) The Contractor shall provide acknowledgment of receipt to the Contracting Officer within three (3) calendar days after receipt of the task order.

(f) If time constraints do not permit issuance of a fully defined task order in accordance with the procedures described in paragraphs (a) through (d), a task order which includes a ceiling price may be issued.

(g) The Contracting Officer may amend tasks in the same manner in which they were issued.

(h) In the event of a conflict between the requirements of the task order and the Contractor's approved task plan, the task order shall prevail.

(End of Clause)

(19) SUPPLEMENTAL TASK ORDERING PROCEDURES (BPA)

(a) When the Government issues a request for a "Task Plan" to the Contractor in accordance with NFS 1852.216-80 entitled "Task Ordering Procedure" clause of this order, the Contractor shall prepare its firm fixed price proposal detailing the labor hours, labor categories and other direct costs required to perform the task order requirements. The Contractor shall use the labor categories and labor rates (which are not to exceed rates) in Attachment B to calculate the proposed estimated cost to perform the task order requirements.

(b) The Contractor agrees that only those appropriate labor rates found in Attachment B shall be used to calculate the proposed firm fixed price for all task orders issued in accordance with the "Task Ordering Procedure" clause. The Contractor's proposed approach/pricing of the representative task set forth in its proposal for award of this contract shall be used as reference by the Contracting Officer in negotiating tasks with the Contractor which is issued under this BPA, but only to the extent portions of a representative task are relevant to portions of a task actually issued.

(End of Text)

(20) (NFS 1852.237-72) ACCESS TO SENSITIVE INFORMATION (JUN 2005)

(a) As used in this clause, "sensitive information" refers to information that a contractor has developed at private expense, or that the Government has generated that qualifies for an exception to the Freedom of Information Act, which is not currently in the public domain, and which may embody trade secrets or commercial or financial information, and which may be sensitive or privileged.

(b) To assist NASA in accomplishing management activities and administrative functions, the Contractor shall provide the services specified elsewhere in this contract.

(c) If performing this contract entails access to sensitive information, as defined above, the Contractor agrees to –

(1) Utilize any sensitive information coming into its possession only for the purposes of performing the services specified in this contract, and not to improve its own competitive position in another procurement.

(2) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.

(3) Allow access to sensitive information only to those employees that need it to perform services under this contract.

(4) Preclude access and disclosure of sensitive information to persons and entities outside of the Contractor's organization.

(5) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in this contract and to safeguard it from unauthorized use and disclosure.

(6) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.

(7) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(d) The Contractor will comply with all procedures and obligations specified in its Organizational Conflicts of Interest Avoidance Plan, which this contract incorporates as a compliance document.

(e) The nature of the work on this contract may subject the Contractor and its employees to a variety of laws and regulations relating to ethics, conflicts of interest, corruption, and other criminal or civil matters relating to the award and administration of government contracts. Recognizing that this contract establishes a high standard of accountability and trust, the Government will carefully review the Contractor's performance in relation to the mandates and restrictions found in these laws and regulations. Unauthorized uses or disclosures of sensitive information may result in termination of this contract for default, or in debarment of the Contractor for serious misconduct affecting present responsibility as a government contractor.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), suitably modified to reflect the relationship of the parties, in all subcontracts that may involve access to sensitive information

(End of Clause)

(21) (NFS 1852.237-73) RELEASE OF SENSITIVE INFORMATION (JUN 2005)

(a) As used in this clause, "sensitive information" refers to information, not currently in the public domain, that the Contractor has developed at private expense, that may embody trade secrets or commercial or financial information, and that may be sensitive or privileged.

(b) In accomplishing management activities and administrative functions, NASA relies heavily on the support of various service providers. To support NASA activities and functions, these service providers, as well as their subcontractors and their individual employees, may need access to sensitive information submitted by the Contractor under this contract. By submitting this proposal or performing this contract, the Contractor agrees that NASA may release to its service providers, their subcontractors, and their individual employees, sensitive information submitted during the course of this procurement, subject to the enumerated protections mandated by the clause at 1852.237-72, Access to Sensitive Information.

(c) (1) The Contractor shall identify any sensitive information submitted in support of this proposal or in performing this contract. For purposes of identifying sensitive information, the Contractor may, in addition to any other notice or legend otherwise required, use a notice similar to the following:
Mark the title page with the following legend:

This proposal or document includes sensitive information that NASA shall not disclose outside the Agency and its service providers that support management activities and administrative functions. To gain access to this sensitive information, a service provider's contract must contain the clause at NFS

1852.237-72, Access to Sensitive Information. Consistent with this clause, the service provider shall not duplicate, use, or disclose the information in whole or in part for any purpose other than to perform the services specified in its contract. This restriction does not limit the Government's right to use this information if it is obtained from another source without restriction. The information subject to this restriction is contained in pages: NONE.

Mark each page of sensitive information the Contractor wishes to restrict with the following legend:

Use or disclosure of sensitive information contained on this page is subject to the restriction on the title page of this proposal or document.

(2) The Contracting Officer shall evaluate the facts supporting any claim that particular information is "sensitive." This evaluation shall consider the time and resources necessary to protect the information in accordance with the detailed safeguards mandated by the clause at 1852.237-72, Access to Sensitive Information. However, unless the Contracting Officer decides, with the advice of Center counsel, that reasonable grounds exist to challenge the Contractor's claim that particular information is sensitive, NASA and its service providers and their employees shall comply with all of the safeguards contained in paragraph (d) of this clause.

(d) To receive access to sensitive information needed to assist NASA in accomplishing management activities and administrative functions, the service provider must be operating under a contract that contains the clause at 1852.237-72, Access to Sensitive Information. This clause obligates the service provider to do the following:

(1) Comply with all specified procedures and obligations, including the Organizational Conflicts of Interest Avoidance Plan, which the contract has incorporated as a compliance document.
(2) Utilize any sensitive information coming into its possession only for the purpose of performing the services specified in its contract.
(3) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.
(4) Allow access to sensitive information only to those employees that need it to perform services under its contract.
(5) Preclude access and disclosure of sensitive information to persons and entities outside of the service provider's organization.
(6) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in its contract and to safeguard it from unauthorized use and disclosure.
(7) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.
(8) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(e) When the service provider will have primary responsibility for operating an information technology system for NASA that contains sensitive information, the service provider's contract shall include the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources. The Security Requirements clause requires the service provider to implement an Information Technology Security Plan to protect information processed, stored, or transmitted from unauthorized access, alteration, disclosure, or use. Service provider personnel requiring privileged access or limited privileged access to these information technology systems are subject to screening using the standard National Agency Check (NAC) forms appropriate to the level of risk for adverse impact to NASA missions. The Contracting Officer may allow the service provider to conduct its own screening, provided the service provider employs substantially equivalent screening procedures.

(f) This clause does not affect NASA's responsibilities under the Freedom of Information Act.

(g) The Contractor shall insert this clause, including this paragraph (g), suitably modified to reflect the relationship of the parties, in all subcontracts that may require the furnishing of sensitive information.

(End of Clause)

(22) (NFS 1852.242-72) OBSERVANCE OF LEGAL HOLIDAYS (AUG 1992) (ALTERNATE II) (SEPT 1989)

(a) The on-site Government personnel observe the following holidays:
New Year's Day
Labor Day
Martin Luther King, Jr.'s Birthday
Columbus Day
President's Day
Veterans Day
Memorial Day
Thanksgiving Day
Independence Day
Christmas Day

Any other day designated by Federal statute, Executive order, or the President's proclamation.

(b) When any holiday falls on a Saturday, the preceding Friday is observed. When any holiday falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not by itself be cause for an additional period of performance or entitlement of compensation except as set forth within the contract.

(c) When the NASA installation grants administrative leave to its Government employees (e.g., as a result of inclement weather, potentially hazardous conditions, or other special circumstances), Contractor personnel working on-site should also be dismissed. However, the contractor shall provide sufficient on-site personnel to perform round-the-clock requirements of critical work

already in process, unless otherwise instructed by the Contracting Officer or authorized representative.

(d) Whenever administrative leave is granted to Contractor personnel pursuant to paragraph (c) of this clause, it shall be without loss to the Contractor. The cost of salaries and wages to the Contractor for the period of any such excused absence shall be a reimbursable item of cost under this contract for employees in accordance with the Contractor's established accounting policy.

(End of Clause)

(23) (NFS 1852.245-71) INSTALLATION-ACCOUNTABLE GOVERNMENT PROPERTY (DEVIATION) (SEPT 2007)

(a) The Government property described in paragraph (c) of this clause may be made available to the Contractor on a no-charge basis for use in performance of this contract. This property shall be utilized only within the physical confines of the NASA installation that provided the property unless authorized by the contracting officer under (b)(1)(iv). Under this clause, the Government retains accountability for, and title to, the property, and the Contractor shall comply with the following:

NASA Procedural Requirements (NPR) 4100, NASA Materials Inventory Management Manual
NASA Procedural Requirements (NPR) 4200, NASA Equipment Management Procedural Requirements
NASA Procedural Requirement (NPR) 4300, NASA Personal Property Disposal Procedural Requirements

Property not recorded in NASA property systems must be managed in accordance with the requirements of FAR 52.245-1.

The Contractor shall establish and adhere to a system of written procedures to assure continued, effective management control and compliance with these user responsibilities. Such procedures must include holding employees liable, when appropriate, for loss, damage, or destruction of Government property.

(b)(1) The official accountable recordkeeping, financial control, and reporting of the property subject to this clause shall be retained by the Government and accomplished within NASA management information systems prescribed by the installation Supply and Equipment Management Officer (SEMO) and Financial Management Officer. If this contract provides for the Contractor to acquire property, title to which will vest in the Government, the following additional procedures apply:

(i) The Contractor's purchase order shall require the vendor to deliver the property to the installation central receiving area.

(ii) The Contractor shall furnish a copy of each purchase order, prior to delivery by the vendor, to the installation central receiving area.

(iii) The Contractor shall establish a record of the property as required by FAR 52.245-1, Government Property, and furnish to the Industrial Property Officer a DD Form 1149, Requisition and Invoice/Shipping Document, (or installation equivalent) to transfer accountability to the Government within 5 working days after receipt of the property by the Contractor. The Contractor is accountable

for all contractor-acquired property until the property is transferred to the Government's accountability.

(iv) Contractor use of Government property at an off-site location and off-site subcontractor use require advance approval of the Contracting Officer and notification of the Industrial Property Officer. The property shall be considered Government furnished and the Contractor shall assume accountability and financial reporting responsibility. The Contractor shall establish records and property control procedures and maintain the property in accordance with the requirements of FAR 52.245-1, Government Property, until its return to the installation. NASA Procedural Requirements related to property loans shall not apply to offsite use of property by contractors.

(2) After transfer of accountability to the Government, the Contractor shall continue to maintain such internal records as are necessary to execute the user responsibilities identified in paragraph (a) of this clause and document the acquisition, billing, and disposition of the property. These records and supporting documentation shall be made available, upon request, to the SEMO and any other authorized representatives of the Contracting Officer.

(c) The following property and services are provided if checked.

__√__(1) Office space, work area space, and utilities. Government telephones are available for official purposes only.

__√__(2) Office furniture.

___(3) Property listed

(ii) If the Contractor acquires property, title to which vests in the Government pursuant to other provisions of this contract, this property also shall become accountable to the Government upon its entry into Government records.

(iii) The Contractor shall not bring to the installation for use under this contract any property owned or leased by the Contractor, or other property that the Contractor is accountable for under any other Government contract, without the Contracting Officer's prior written approval.

___ (4) Supplies from stores stock.

___ (5) Publications and blank forms stocked by the installation.

___(6) Safety and fire protection for Contractor personnel and facilities.

__√__ (7) Installation service facilities: __Agency Consolidated End-User Services (ACES)__

___ (8) Medical treatment of a first-aid nature for Contractor personnel injuries or illnesses sustained during on-site duty.

__√__(9) Cafeteria privileges for Contractor employees during normal operating hours.

___ (10) Building maintenance for facilities occupied by Contractor personnel.

___ (11) Moving and hauling for office moves, movement of large equipment, and delivery of supplies. Moving services may be provided on-site, as approved by the Contracting Officer.

(End of Clause)

(24) (NFS 1852.245-74) CONTRACTOR ACCOUNTABLE ON-SITE GOVERNMENT PROPERTY (MARCH 1989)

(a) In performance of work under this contract, certain Government property identified in the contract shall be provided to the Contractor on a no-charge-for-use basis by the installation's Supply and Equipment Management Officer. That property shall be utilized in the performance of this contract at the installation that provided the property or at such other installations or locations as may be specified elsewhere in this contract. The Contractor assumes accountability and user responsibilities for the property.

(b) Government property provided shall in every respect be subject to the provisions of the FAR 52.245 Government property clause of this contract. In addition, the contractor is responsible for managing this property in accordance with the guidelines provided by the installation's Supply and Equipment Management Officer or any other formally designated representatives of the Contracting Officer. The guidelines include but are not limited to requiring the Contractor to--
(1) Use economic order quantity (EOQ) methods for routine stock replenishment;
(2) Utilize the Federal Cataloging System;
(3) Comply with shelf-life requirements;
(4) Provide for accountability and control (using the NASA Equipment Management System (NEMS)) of all equipment costing $1000 and over, plus that equipment designated as "sensitive";
(5) Provide for physical inventory of all controlled equipment at least every 3 years;
(6) Provide for sample inventories of materials plus complete inventories every 5 years;
(7) Conduct walk-through utilization inspections;
(8) Screen NEMS before acquiring any equipment costing $1000 or over, plus equipment designated by the installation as sensitive and costing $500 and over;
(9) Support the Equipment Acquisition Document (EAD) process; and
(10) Use Government sources as the first source of supply.
(c) Data requirements relating to the guidelines in paragraph (b) of this clause are specified under Section F, Deliveries or performance.

(End of Clause)

(25) (NFS 1852.245-75) PROPERTY MANAGEMENT CHANGES (DEVIATION) (JAN 2011)

(a) The Contractor shall submit any changes to standards and practices used for management and control of Government property under this contract to the assigned property administrator prior to making the change whenever the change--

(1) Employs a standard that allows increase in thresholds or changes the timing for reporting loss, damage, or destruction of property;

(2) Alters physical inventory timing or procedures;

(3) Alters recordkeeping practices;

(4) Alters practices for recording the transport or delivery of Government property; or

(5) Alters practices for disposition of Government property.

(End of clause)

(26) (NFS 1852.245-82) OCCUPANCY MANAGEMENT REQUIREMENTS (JAN 2011)

(a) In addition to the requirements of the clause at FAR 52.245-1, Government Property, as included in this contract, the Contractor shall comply with the following in performance of work in and around Government real property:

(1) NPD 8800.14, Policy for Real Property Management.
(2) NPR 8831.2, Facility Maintenance Management.

(b) The Contractor shall obtain the written approval of the Contracting Officer before installing or removing Contractor-owned property onto or into any Government real property or when movement of Contractor-owned property may damage or destroy Government-owned property. The Contractor shall restore damaged property to its original condition at the Contractor's expense.

(c) The Contractor shall not acquire, construct or install any fixed improvement or structural alterations in Government buildings or other real property without the advance, written approval of the Contracting Officer. Fixed improvement or structural alterations, as used herein, means any alteration or improvement in the nature of the building or other real property that, after completion, cannot be removed without substantial loss of value or damage to the premises. Title to such property shall vest in the Government.

(d) The Contractor shall report any real property or any portion thereof when it is no longer required for performance under the contract, as directed by the Contracting Officer.

(End of Clause)

(27) (HQ 52.204-98) ONSITE CONTRACTOR PERSONNEL – IDENTIFICATION, REPORTING, AND CHECKOUT PROCEDURES (JAN 2007)

(a) The Contractor's designated representative for the purposes of this clause is the Contractor's Project Manager. The Contractor shall notify the Headquarters Chief of Security and the Contracting Officer's Technical Representative of the Project Manager's identity within fifteen (15) calendar days of award of this contract.
(b) In accordance with FAR 52.204-9, Personal Identity Verification of Contractor Personnel, the Contractor shall follow the steps in Attachment H, Personal Identity Verification (PIV) Card Issuance and Re-issuance Procedures, for each contract employee (prime and subcontractor) who shall have physical access to a NASA-controlled facility (also referred to as "onsite") or access to a Federal information system. The Contractor must apply for permanent NASA Headquarters PIV credential for those contract employees who will be employed by the Contractor onsite for at least six months. The Headquarters Security Office will consider permanent PIV credentials for other employees of the Contractor on a case-by-case basis, such as employees that are not resident onsite, but must frequently visit.
(c) The Contractor's Project Manager shall submit written notification to the Contracting Officer's Technical Representative and the Headquarters Chief of Security immediately about any Contractor employee who was issued a Headquarters PIV credential or who was granted temporary access to be on-site: (1) who is no longer employed by the Contractor, or (2) who will no longer be working onsite under this contract.
(d) The Contractor shall ensure that all personnel who have NASA Headquarters issued credentials, keys or other property who leave the Contractor's employ or that no longer work onsite, process out through the Headquarters Security Office. Any such Contractor employees must return all Headquarters issued identification or credentials and any Government property no later than the last day of their employment. The Contractor shall establish appropriate procedures and controls to ensure this is accomplished. Failure to comply may result in the exercise of Government rights to

limit and control access to Government premises, including denial of access and invalidation of NASA issued PIV credentials.

(End of Clause)

(28) (HQ 52.204-99) GOVERNMENT PREMISES-PHYSICAL AND LOGICAL ACCESS AND COMPLIANCE WITH PROCEDURES (JAN 2007)

a)(1) The Contractor must apply for NASA Headquarters Personal Identity Verification (PIV) credential issued by the Headquarters Security Office for those employees that will be employed by the Contractor and that will be resident or access NASA Headquarter locations, or NASA cyber resources for more than six (6) months. The Headquarters PIV credentials will be issued for no longer than the applicable contract period in effect at the time, not to exceed 5-years, and will require renewal for each subsequent contract period within which the Contractor employee will be employed. Based on NASA policies and procedures for background investigations and position risk/sensitivity determination, a minimum of National Agency Check with Written Inquiries (NACI) will be required for credential renewal. Other Contractor personnel who are to be at the Headquarters location(s) or will be accessing NASA cyber resources for less than six (6) months are to be identified by the Contractor for approval and registered on an access list under the control of the Headquarters Security Office. All personnel must conspicuously display the Headquarters PIV credential above the waistline on the outermost garment, and must comply with any and all requirements applicable to PIV credential in effect at Headquarters. In accordance with FAR 52.204-9, Personal Identity Verification of Contractor Personnel, the Contractor shall follow the steps prescribed in **Attachment H,** Personal Identity Verification (PIV) Card Issuance Procedures to apply for each contract employee (prime and subcontractor) who shall have physical access to a NASA-controlled facility (also referred to as "onsite") or access to a Federal information system.
(2) Visits by foreign nationals to, for, or on behalf of the Contractor, are restricted and must be necessary for the performance of the contract and concurred in by the Contracting Officer or by the Contracting Officer's Technical Representative. Approval of such visits must be approved in advance in accordance with NASA Procedural Requirements, NPR 1371.2A, Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities w/Change 1 (3/29/04); and NASA Policy Directive, NPD 1371.5A, Coordination and Authorization of Access by Foreign Nationals and Foreign Representatives to NASA (Revalidated 3/29/04), http://nodis.hq.nasa.gov. The Contractor may get further information about visits by foreign nationals by contacting the NASA Headquarters International Visits Coordinator located in the Headquarters Security Office. (3) Access to the Headquarters locations may be changed or adjusted in response to threat conditions or special situations.
(b) While on Government premises, the Contractor shall comply with requirements governing the conduct of personnel and the operation of the Headquarters locations. These requirements are set forth in NASA-wide or Headquarters installation directives, and procedural requirements, and announcements that can be found at http://nodis.hq.nasa.gov, and/or which will be provided to the Contractor as necessary by the Contracting Officer's Technical Representative, the Contracting Officer, or the Headquarters Chief of Security.(c) The Contractor may not use official Government envelopes or other Government identified mailing containers bearing any sort of Government indicia such as "eagle" emblems in lieu of postage stamps or mailing envelopes or containers bearing NASA logos. The Contractor also may not use the Government mail system to mail anything outside of the Headquarters locations. Contractors found in violation could be liable for a

fine of $300 per piece of indicia mail used. Otherwise, the Contractor is allowed to use the internal Headquarters interoffice mail system to send documents **within the Headquarters locations or to other NASA Centers or NASA facilities** the extent necessary for purposes of implementing the terms of this contract and communicating contract related business to its employees at the Headquarters locations, and to communicate contract related business to NASA officials including, but not limited to, the Contracting Officer, the Contracting Officer's Technical Representative, the Headquarters Chief of Security, Accounting Office staff, and the NASA Headquarters International Visits Coordinator.

(End of Clause)

(29) 1852.223-70 SAFETY AND HEALTH (APRIL 2002)

(a) Safety is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. NASA's safety priority is to protect: (1) the public, (2) astronauts and pilots, (3) the NASA workforce (including contractor employees working on NASA contracts), and (4) high-value equipment and property.

(b) The Contractor shall take all reasonable safety and occupational health measures in performing this contract. The Contractor shall comply with all Federal, State, and local laws applicable to safety and occupational health and with the safety and occupational health standards, specifications, reporting requirements, and any other relevant requirements of this contract.

(c) The Contractor shall take, or cause to be taken, any other safety, and occupational health measures the Contracting Officer may reasonably direct. To the extent that the Contractor may be entitled to an equitable adjustment for those measures under the terms and conditions of this contract, the equitable adjustment shall be determined pursuant to the procedures of the changes clause of this contract; provided, that no adjustment shall be made under this Safety and Health clause for any change for which an equitable adjustment is expressly provided under any other clause of the contract.

(d) The Contractor shall immediately notify and promptly report to the Contracting Officer or a designee any accident, incident, or exposure resulting in fatality, lost-time occupational injury, occupational disease, contamination of property beyond any stated acceptable limits set forth in the contract Schedule; or property loss of $25,000 or more, or Close Call (a situation or occurrence with no injury, no damage or only minor damage (less than $1,000) but possesses the potential to cause any type mishap, or any injury, damage, or negative mission impact) that may be of immediate interest to NASA, arising out of work performed under this contract. The Contractor is not required to include in any report an expression of opinion as to the fault or negligence of any employee. In addition, service contractors (excluding construction contracts) shall provide quarterly reports specifying lost-time frequency rate, number of lost-time injuries, exposure, and accident/incident dollar losses as specified in the contract Schedule.

(e) The Contractor shall investigate all work-related incidents, accidents, and Close Calls, to the extent necessary to determine their causes and furnish the Contracting Officer a report, in such form as the Contracting Officer may require, of the investigative findings and proposed or completed corrective actions.

(f)(1) The Contracting Officer may notify the Contractor in writing of any noncompliance with this clause and specify corrective actions to be taken. When the Contracting Officer becomes aware

of noncompliance that may pose a serious or imminent danger to safety and health of the public, astronauts and pilots, the NASA workforce (including contractor employees working on NASA contracts), or high value mission critical equipment or property, the Contracting Officer shall notify the Contractor orally, with written confirmation. The Contractor shall promptly take and report any necessary corrective action.

(2) If the Contractor fails or refuses to institute prompt corrective action in accordance with subparagraph (f)(1) of this clause, the Contracting Officer may invoke the stop-work order clause in this contract or any other remedy available to the Government in the event of such failure or refusal.

(g) The Contractor (or subcontractor or supplier) shall insert the substance of this clause, including this paragraph (g) and any applicable Schedule provisions and clauses, with appropriate changes of designations of the parties, in all solicitations and subcontracts of every tier, when one or more of the following conditions exist:

(1) The work will be conducted completely or partly on premises owned or controlled by the Government.

(2) The work includes construction, alteration, or repair of facilities in excess of the simplified acquisition threshold.

(3) The work, regardless of place of performance, involves hazards that could endanger the public, astronauts and pilots, the NASA workforce (including Contractor employees working on NASA contracts), or high value equipment or property, and the hazards are not adequately addressed by Occupational Safety and Health Administration (OSHA) or Department of Transportation (DOT) regulations (if applicable).

(4) When the Contractor (or subcontractor or supplier) determines that the assessed risk and consequences of a failure to properly manage and control the hazard(s) warrants use of the clause.

(h) The Contractor (or subcontractor or supplier) may exclude the provisions of paragraph (g) from its solicitation(s) and subcontract(s) of every tier when it determines that the clause is not necessary because the application of the OSHA and DOT (if applicable) regulations constitute adequate safety and occupational health protection. When a determination is made to exclude the provisions of paragraph (g) from a solicitation and subcontract, the Contractor must notify and provide the basis for the determination to the Contracting Officer. In subcontracts of every tier above the micro-purchase threshold for which paragraph (g) does not apply, the Contractor (or subcontractor or supplier) shall insert the substance of paragraphs (a), (b), (c), and (f) of this clause).

(i) Authorized Government representatives of the Contracting Officer shall have access to and the right to examine the sites or areas where work under this contract is being performed in order to determine the adequacy of the Contractor's safety and occupational health measures under this clause.

(j) The contractor shall continually update the safety and health plan when necessary. In particular, the Contractor shall furnish a list of all hazardous operations to be performed, and a list of other major or key operations required or planned in the performance of the contract, even though not deemed hazardous by the Contractor. NASA and the Contractor shall jointly decide

which operations are to be considered hazardous, with NASA as the final authority. Before hazardous operations commence, the Contractor shall submit for NASA concurrence --

(1) Written hazardous operating procedures for all hazardous operations; and/or

(2) Qualification standards for personnel involved in hazardous operations.

(End of clause)

(30) RESERVED

(31) 52.227-14 RIGHTS IN DATA-GENERAL (52.227-14)(DEC 2007) as modified by NASA FAR Supplement 1852.227-14—ALTERNATE II (DEC 2007) AND ALTERNATE III (DEC 2007)

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

"Computer database" or "database means" a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"-

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics,

and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 403(8)).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in-

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to-

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright-

(1) Data first produced in the performance of this contract.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor-

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except-

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(i) The Contractor agrees not to establish claim to copyright, publish or release to others any computer software first produced in the performance of this contract without the Contracting Officer's prior written permission.

(ii) If the Government desires to obtain copyright in computer software first produced in the performance of this contract and permission has not been granted as set forth in paragraph (d)(3)(i) of this clause, the Contracting Officer may direct the contractor to assert, or authorize the assertion of, claim to copyright in such data and to assign, or obtain the assignment of, such copyright to the Government or its designated assignee.

(iii) Whenever the word "establish" is used in this clause, with reference to a claim to copyright, it shall be construed to mean "assert".

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 253d, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore

the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor-

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may-

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software.

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall-

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) Notwithstanding paragraph (g)(1) of this clause, the contract may identify and specify the delivery of limited rights data, or the Contracting Officer may require by written request the delivery of limited rights data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the Contractor shall affix the following "Limited Rights Notice" to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with the notice:

Limited Rights Notice (Dec 2007)

(a) These data are submitted with limited rights under Government Contract No. _____ (and subcontract _____, if appropriate). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure:

(i) Use (except for manufacture) by support service contractors.

(ii) Evaluation by nongovernment evaluators.

(iii) Use (except for manufacture) by other contractors participating in the Government's program of which the specific contract is a part.

(iv) Emergency repair or overhaul work.

(v) Release to a foreign government, or its instrumentalities, if required to serve the interests of the U.S. Government, for information or evaluation, or for emergency repair or overhaul work by the foreign government.

(vi) or any other legitimate government use

(b) This notice shall be marked on any reproduction of these data, in whole or in part.

(End of notice)

(4)(i) Notwithstanding paragraph (g)(1) of this clause, the contract may identify and specify the delivery of restricted computer software, or the Contracting Officer may require by written request the delivery of restricted computer software that has been withheld or would otherwise be entitled to be withheld. If delivery of that computer software is required, the Contractor shall affix the following "Restricted Rights Notice" to the computer software and the Government will treat the computer software, subject to paragraphs (e) and (f) of this clause, in accordance with the notice:

Restricted Rights Notice (Dec 2007)

(a) This computer software is submitted with restricted rights under Government Contract No. _____ (and subcontract _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this notice or as otherwise expressly stated in the contract.

(b) This computer software may be-

(1) Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation to which the computer(s) may be transferred;

(2) Used or copied for use with a backup computer if any computer for which it was acquired is inoperative;

(3) Reproduced for safekeeping (archives) or backup purposes;

(4) Modified, adapted, or combined with other computer software, *provided* that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights;

(5) Disclosed to and reproduced for use by support service Contractors or their subcontractors in accordance with paragraphs (b)(1) through (4) of this notice; and

(6) Used or copied for use with a replacement computer and other legitimate government use.

(c) Notwithstanding the foregoing, if this computer software is copyrighted computer software, it is licensed to the Government with the minimum rights set forth in paragraph (b) of this notice.

(d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

(e) This notice shall be marked on any reproduction of this computer software, in whole or in part.

(End of notice)

(ii) Where it is impractical to include the Restricted Rights Notice on restricted computer software, the following short-form notice may be used instead:

Restricted Rights Notice Short Form (Jun 1987)

Use, reproduction, or disclosure is subject to restrictions set forth in Contract No. _____ (and subcontract, if appropriate) with _____ (name of Contractor and subcontractor).

(End of notice)

(iii) If restricted computer software is delivered with the copyright notice of 17 U.S.C. 401, it will be presumed to be licensed to the Government without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

(h) *Subcontracting.* The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of Clause)

(32) 52.227-17 RIGHTS IN DATA—SPECIAL WORKS (DEC 2007)*

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

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of Rights.

(1) The Government shall have—

(i) Unlimited rights in all data delivered under this contract, and in all data first produced in the performance of this contract, except as provided in paragraph (c) of this clause.

(ii) The right to limit assertion of copyright in data first produced in the performance of this contract, and to obtain assignment of copyright in that data, in accordance with paragraph (c)(1) of this clause.

(iii) The right to limit the release and use of certain data in accordance with paragraph (d) of this clause.

(2) The Contractor shall have, to the extent permission is granted in accordance with paragraph (c)(1) of this clause, the right to assert claim to copyright subsisting in data first produced in the performance of this contract.

(c) Copyright—

(1) Data first produced in the performance of this contract.

(i) The Contractor shall not assert or authorize others to assert any claim to copyright subsisting in any data first produced in the performance of this contract without prior written permission of the Contracting Officer. When copyright is asserted, the Contractor shall affix the appropriate copyright notice of 17 *U.S.C. 401 or 402* and acknowledgment of Government sponsorship (including contract number) to the data when delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. The Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license for all delivered data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

(ii) If the Government desires to obtain copyright in data first produced in the performance of this contract and permission has not been granted as set forth in paragraph (c)(1)(i) of this clause, the Contracting Officer shall direct the Contractor to assign (with or without registration), or obtain the assignment of, the copyright to the Government or its designated assignee.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract and that contain the copyright notice of 17 U.S.C. 401 or 402, unless the Contractor identifies such data and grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

(d) *Release and use restrictions.* Except as otherwise specifically provided for in this contract, the Contractor shall not use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.

(e) *Indemnity.* The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred

as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies.

(End of clause)

***The data specified in the table on the subsequent page is applicable to Item (32). In addition, the Government will retain unlimited rights to the documentation and data required for successfully passing each of the required reviews in NASA Procedural Requirements (NPR) 7120.99. Such reviews include, but may not be limited to: System Concept Review; Systems Requirements Review; Preliminary Design Review; Critical Design Review; Test Readiness Review; Operational Readiness Review; Project Completion Review; and Decommissioning Review. All other data not referenced that is developed and/or delivered under this BPA shall be governed by Item (31) FAR 52.227-14 RIGHTS IN DATA-GENERAL (52.227-14)(DEC 2007) as modified by NASA FAR SUPPLEMENT 1852.227-14—ALTERNATE II (DEC 2007) and ALTERNATE III (DEC 2007).**

(33) (GSFC 52.232-95) INVOICES - SUBMISSION OF (AUG 2008)

(a) Invoices shall be prepared in accordance with the Prompt Payment clause of this contract and submitted to the NASA Shared Services Center (NSSC), Financial Management Division (FMD) – Accounts Payable, Bldg 1111, C. Road, Stennis Space Center, MS 39529, Email: NSSC-AccountsPayable@nasa.gov. For purposes of the Prompt Payment Act, the above office is considered to be the "Designated Billing Office" and the "Designated Payment Office".

(b) If the terms are F.O.B. plant with "plus transportation charges allowed", the invoice must be supported by a receipted freight bill, express receipt, or parcel post receipt, evidencing the correctness of the amount paid and claimed. If the amount is less than $100 per shipment and receipts are not available, the invoice will be accepted and payment made, provided it contains a certificate by the supplier, that transportation charges were in fact paid by the supplier, that receipts were not available, and lists the destination, weight, name of carrier, and the amount claimed. The availability of this certification is not a waiver of the requirements for receipted transportation bills, and is to be used only when receipts are not available. Bill of lading number and weight of shipment shall be shown for shipments made on Government bill of lading.

(End of Clause)

(34) (GSFC 52.246-93) ACCEPTANCE—LOCATION(S) (APR 2008)

(a) The Contracting Officer or authorized representative will accomplish acceptance at the following location(s):

Item	Location	Authorized Representative
Deliverables and services as specified in the SOW and Task Orders	**As Specified on Individual Task Orders**	**COR**

(b) The Contracting Officer reserves the right to designate other Government agents as authorized representatives. The Contractor will be notified by a written notice or by a copy of the delegation letter if other agents are authorized.

(End of Clause)

(35) (GSFC 52.246-102) INSPECTION SYSTEM RECORDS (OCT 1988)

(a) The Contractor shall maintain records evidencing inspections in accordance with the Inspection clause of this contract for three (3) years after delivery of all items and/or completion of all services called for by the contract.

(End of Clause)

(36) (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 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

(End of Clause)

(37) (FAR 52.217-9) OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

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

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

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

(End of Clause)

(38) OPTION TO EXTEND

In accordance with FAR clause 52.217-9, "Option to Extend the Term of the Contract" of this contract, the contracting officer may exercise the following option(s) by issuance of a unilateral contract modification. Options exercised shall be in accordance with the following:

Option	Period of Performance
1	Twelve (12) months commencing after the end of the basic period
2	Twelve (12) months commencing after the end of Option Period 1
3	Twelve (12) months commencing after the end of Option Period 2
4	Twelve (12) months commencing after the end of Option Period 3

(End of Text)

(39) LIST OF ATTACHMENTS

The following documents are attached hereto and made a part of this contract:

Attachment	Description	No. of Pages	Date
A	WESTPRIME Statement of Work	9	07/20/2012
B	Loaded Labor Rates Matrix	22-24 of the Offeror's Price Proposal, Volume 3***	09/07/2012
C	I3P Cross Functional Performance Work Statement (PWS)	83	07/20/2012
D	IT Security Plan and Management Plan	Submission due within 30 days of effective date	TBD*
E	OCI Avoidance Plan	Submission due within 15 days of effective date	TBD*
F	IT Security ADL	4	01/2012
G	Position Descriptions	25 – 61 of the Offeror's Price Proposal, Volume 3	09/07/2012
H	Personal Identity Verification	4	07/20/2012
I	Safety & Health Plan	Attachment 1 of the Offeror's Technical Proposal, Volume 1	09/07/2012
J	DD Form 254 – Contract Security Classification Specification	Submission due with Signature Copy of BPA	12/20/2012

***TBD = "To Be Determined"**
****TBP = "To Be Proposed"**
*****GSA Schedule Contract Expires 02/03/2014. Orders will not be issued beyond the approved GSA Schedule Contract expiration date.**

(End of Text)

(END OF BPA)

ATTACHMENT A

STATEMENT OF WORK

07/20/2012

Introduction

The primary purpose of this requirement is to establish the consolidated and integrated web service delivery capability for Sandbox, Development/Test, Staging/Pre-Production and Production environment that will streamline the migration, implementation and support of current and future NASA websites and web applications to the Cloud. Public Cloud will be the preferred environment for public websites and a hybrid Cloud environment will be required for web applications and internal applications. Appendix B lists the current Applications and Websites. All Appendices and other technical documents can be accessed at http://i3p.nasa.gov/document_file_home.cfm under the category WESTPRIME.

WEB Services Goals and Objectives:

The NASA Office of the Chief Information Officer (OCIO) has established the following principles to guide tactical decisions and planning now and in the future:

- MISSION ENABLING: IT at NASA serves to enable NASA's mission.
- INTEGRATED: NASA will implement IT that enables integration of business (mission) processes and information across organizational boundaries.
- EFFICIENT: NASA will implement IT to achieve efficiencies and ensure that IT is efficiently implemented.
- SECURE: NASA will implement and sustain secure IT solutions.

In direct support of these key principles, the following NASA IT goals and specific web services objectives were established for the NASA Web Strategy:

Goal 1: Transform NASA's IT infrastructure and application services to better meet evolving stakeholder needs and support mission success

Objectives:

- Work with missions in understanding and meeting their web needs
- Adopt services in close cooperation with customer base
- Deploy solutions that are standards based and interoperable
- Quickly adopt industry proven technologies and practices

Goal 2: Enhance and strengthen IT Security and Cyber security to ensure the integrity, availability, and confidentiality of NASA's critical data and IT assets.

Objectives:

- Provide a secure, shared web infrastructure and environment
- Provide guidance in coding standards and libraries that minimize security risks
- Perform periodic scans of web assets to assess vulnerabilities
- Collaborate with NASA Security Operation Center to improve security of core web platform
- Provide standardized, coordinated rapid response to Web Security issues.

Goal 3: Identify, test, and adopt new information technology that will make NASA's missions more capable and affordable.

Objectives:

- Increase cost efficiencies by using shared services
- Prototype innovative technologies
- Leverage open source to drive down cost of software
- Migrate services to cloud, where practical and cost effective
- Partner with private industry to provide services that are innovative and secure

Goal 4: Provide enterprise resources and processes that foster mission success and allow NASA to attract and retain a highly performing IT workforce.

Objectives:

- User friendly and self serviced
- Employ the latest technologies that missions need
- Balance autonomy and governance
- Create and utilize agile contractual vehicles

WEB Environment Current State:

NASA is comprised of 10 Centers plus several satellite facilities that are geographically distributed throughout the United States. Each Center generally is designing or operating one or more missions or programs. Often, each of these endeavors has its own web infrastructure that is used internally within the mission or program for collaboration amongst the NASA workforce and externally with academia and industry partners. Frequently, custom web applications are built to assist in the design or operation of these missions. In addition, missions will often publish information to the public under its own auspices. These sites are extremely diverse, in that they have a wide variety of audiences, uses and technologies. The different requirements for these services have resulted in a Web environment that is highly autonomous but inconsistent in terms of technology, management, security and information search capabilities. In addition, cross-functional services such as enterprise search are unavailable and complex to implement.

WEB Services Target State:

The target state for web services is to provide a consistent, capable and agile, cloud-based enterprise infrastructure that provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) for internal and external web applications and sites using an interoperable, standards-based and secure environment. All web content development and web application development will be done using other support contract vehicles. Vendors will provide the integrator and Cloud Broker Role as defined in NIST Special Publication 500-292 "NIST Cloud Computing Reference Architecture". http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505

To achieve the goals above, the NASA OCIO will offer a diverse set of services (Appendic C: Figure 1). By offering choices, NASA OCIO will provide an incentive to the NASA community for using this shared service model. The OCIO will also ensure

that the selected tools adhere to a set of guiding principles and standards that meet the OCIO application and web services goals. Guiding principles are as follows:

1. We will strive for vendor independence through the use of open source software.
2. We will prefer Commercial Off the Shelf (COTS), Government Off the Shelf (GOTS) and Open Source solutions to custom-built solutions. This includes cloud offerings.
3. Open standards based solutions will be utilized over closed proprietary solutions.
4. All applications will expose their data and functionality through service interfaces.
5. At a minimum, data access services should be provided by RESTful technologies.
6. Applications that require authentication will integrate with Agency authentication services.

   In terms of the exact nature of the services, the OCIO anticipates providing several choices in each of the service areas. A sample depiction of possible platforms to be offered is shown in Appendix C: Figure 2. Software services shall include multiple choices for CMS, Video Streaming, and Collaboration etc. Appendix C: Figure 3 illustrates how the requirements in the SOW will integrate into the NASA Enterprise Web Environment.

1 General Scope

1.1 The Contractor shall provide NASA with an agency-wide, cloud-based, hosting capability to create maintain and manage websites, web applications and associated ancillary services. Those services shall include content management, search, web analytics, streaming media, and, collaborative tools such as blogs and wikis.

1.2 The Contractor shall perform the following goals of the WESTPRIME contract:

- 1.2.1 Provide web services that meet the needs of NASA's diverse web community.
- 1.2.2 Provide technology refresh and apply industry best practices.
- 1.2.3 Improve agility in adoption of tools and implementation of services.
- 1.2.4 Provide diversity of options for users while managing cost and scope.

1.3 The Contractor shall support some internal-facing applications and websites, such as www.insidenasa.nasa.gov, Space Act Agreement Maker, and the NASA Engineering Network (NEN), which have internal and external users. Appendix B provides an inventory of web sites and Applications

1.4 The WESTPRIME contract is one of five contracts under the Agency Chief Information Officer's Information Technology Infrastructure Integration Program (I3P). The Contractor shall collaborate with the other I3P contractors where WESTPRIME services need to be integrated with those other contracts. For example, the WESTPRIME Contractor shall provide Tier 2 and Tier 3 Support Services, integrated with the Enterprise Service Desk to be provided by NASA at the NASA Shared Services Center.

1.5 The Contractor shall support NASA's efforts to use Information Technology Infrastructure Library, version 3 (ITIL V3), lifecycle processes.

2 General Requirements

2.1 The Contractor shall provide Platform as a Service (PaaS), and Software as a Service (SaaS) for internal and external websites and web applications. Infrastructure as a Service (IaaS) will be provided to support the PaaS and SaaS. Services provided collectively in IaaS, PaaS, and SaaS shall be referred to as the **"offerings"** henceforth.

2.2 The Contractor shall provide the Integrator/Cloud Broker Role as defined in NIST Special Publication 500-292 "NIST Cloud Computing Reference Architecture: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505.

2.3 The Contractor shall integrate security into each layer of the offerings so that the offerings have full Authority to Operate and provide continuous monitoring to effectively manage information systems security.

2.4 The Contractor shall be well versed in agile processes.

2.5 The Contractor shall provide ongoing technical design and implementation support for new elements of sites provisioned through this contract as they are created or incorporated within the existing overarching design

2.6 The Contractor shall use industry-standard components and processes, as demonstrated by the use of those components and processes by industry leaders, in fulfillment of these requirements. Exceptions to using industry-standards components and processes are approved by the Contracting Officers Representative (COR).

2.7 The Contractor shall use technologies in the following order: free open source software (FOSS), Open Source, GOTS,COTS and finally customized development.

2.8 The Contractor shall use NASA specified authentication services to authenticate users to NASA systems that require access control.

2.9 The Contractor shall provide the capability to authenticate users external to NASA to all systems within this contract.

2.10 The Contractor shall be responsible for cost-effective and efficient transition of the NASA shared public web infrastructure to a subsequent contractor at the completion of the contract.

2.11 The contractor shall plan for and implement technology innovation throughout the environment and over the life of the contract to reduce NASA's costs and increase productivity and customer satisfaction.

2.12 The contractor shall support NASA's overall I3P program by coordinating and collaborating with contractors on other contracts to optimize service to NASA users and provide enhanced services to the public, while minimizing duplication of effort, leveraging innovative technologies to maximize cost effectiveness to NASA, and reducing gaps in services.

2.13 The contractor shall provide only tools that are fully functional through a cross-platform web interface that do not require additional software be loaded onto a user's computer and that complies with NASA Standard 2804. *Minimum Interoperability Software Suite.*

3 General Administration – Contractor shall manage all systems and services in compliance with Federal laws, rules, regulations and NASA Policies and Standards.

3.1 **Policy Compliance**

3.1.1 The contractor shall manage all systems and services provided under this contract in compliance with federal laws and regulations and NASA policy, including but not limited to:

3.1.1.1 NASA Policy Directive and NASA Procedural Requirement 1440, "*Records Management.*"

3.1.1.2 NASA Policy Directive and NASA Procedural Requirement 2810, "*Information Technology Security.*"

3.1.1.3 Section 508 of the Rehabilitation Act of 1973 for Electronic and Information Technology, per Subpart B - Technical Standards, Web-based Intranet and Internet Information and Applications (1194.22) parameters and guidelines.

3.1.1.4 NASA's Privacy Policy: NASA Procedural Requirement 1382.1, "*NASA Privacy Procedural Requirements,*" and NASA Policy Directive 1382.17H.

3.1.1.5 NASA Software Engineering Requirements, NASA Policy Directive 7150.2.

3.1.1.6 Compliance with Internet Protocol version 6 (IPv6) in Acquiring Information Technology

3.1.1.6.1 This contract involves the acquisition of Information Technology (IT) that uses Internet Protocol (IP) technology. The contractor shall ensure that (1) all deliverables that involve IT that uses IP (products, services, software, etc.) comply with IPv6 standards and interoperate with both IPv6 and IPv4 systems and products; and (2) it has IPv6 technical support for fielded product management, development and implementation available. If the contractor plans to offer a deliverable that involves IT that is not initially compliant, the contractor shall (1) obtain the Contracting Officer's approval before starting work on the deliverable; and (2) have IPv6 technical support for fielded product management, development and implementation available.

3.1.1.7 NASA Standard 2821, "*Audio and Video Standards for Internet Resources*"

3.1.1.8 NASA Draft Standard, "*Still and Motion Imagery Metadata Standard*"

3.2 Communications and outreach – The Contractor shall work with the OCIO on communication and outreach including but not limited to activities such as:

3.2.1 Written and oral presentations to stakeholders on system functionality

3.2.2 Written and oral presentations on new services

3.2.3 Written and Oral dissemination of notices to NASA community on web services.

4 Project Management

4.1.1 The Contractor shall manage projects under this contract in accordance with NASA Interim Directive 7120.99.

4.1.2 The Contractor shall document all services, tools, information architecture, processes, and configuration management processes and policies used to manage this task and provide documentation to NASA.

5 Help and Service Support

5.1.1 The Contractor shall integrate its Tier 2 and Tier 3 help desk support, incident response, and problem-management and service-ordering systems with NASA's I3P Enterprise Service Desk, as described in NASA's I3P Cross-Functional Performance Work Statement and align them with I3P ITIL processes.

5.2 NASA Customer Feedback

5.2.1 The Contractor shall assist the Government in reviewing the customer Feedback and developing remediation strategies for issues and unsatisfactory feedback.

5.3 Service Ordering

5.3.1 The Contractor shall integrate with the NASA Enterprise Service Request System (ESRS) so that orders for services are placed with the Enterprise Service Request System.

5.4 Performance Metric

5.4.1 The Contractor shall support NASA in the development of the performance metrics for customer satisfaction.

6 End User Training

6.1 The Contractor shall utilize SATERN for any and all training offered to NASA employees in performance of this requirement. NASA operates and maintains an online training system for all NASA Employees and contractors called SATERN (http://satern.nasa.gov), which provides the opportunity to implement standard training processes across the Agency and ease of delivery and administration of training courses and schedules. For all courses, instructor led or online/self-paced, this system is used to schedule, register and record results of courses offered by Agency organizations, programs, and projects. If desired, the system can also be used to deliver Sharable Content Object Reference Model (SCORM)-based online/self-paced courses and record test scores. See the library for links to SATERN information.

7 Availability Requirements

7.1 General Availability Requirements

7.1.1 Availability, as defined in the glossary, shall be measured for each contract week from 12:01 a.m. Eastern time Sunday through midnight Eastern Time Saturday.
7.1.2 The Contractor shall meet the availability performance metric as defined in Availability options in Section 7.2.
7.1.3 The failure of any component system subject to the availability metric shall be deemed an overall failure to meet that metric.

7.2 Service Level for Availability

7.2.1 The Contractor shall provide three offerings of availability for sites and services in this infrastructure as defined in the applicable orders.
- 7.2.1.1 99.995% - For purposes of this calculation, negotiated planned downtime may be excluded from the calculation.
- 7.2.1.2 99.95% - For purposes of this calculation, negotiated planned downtime may be excluded from the calculation.
- 7.2.1.3 99.5% - For purposes of this calculation, negotiated planned downtime may be excluded from the calculation.

7.3 Bandwidth Management

7.3.1 The Contractor shall provide bandwidth for all websites and web applications hosted under this contractor and shall provide innovative solutions for bandwidth busting.
7.3.2 The Contractor shall develop a plan to provide additional needed bandwidth as required.

7.4 Delivery capabilities for live and on-demand video streaming

7.4.1 The Contractor shall provide streaming of live and stored content in industry-standard cross-platform format(s) designated by NASA (e.g., Adobe Flash, HTML5 and HTTP Live Streaming) from NASA or NASA-approved non-NASA sources in a manner compliant with NASA Std 2821 *Audio and Video Standards for Internet Resources*.
7.4.2 Contractor shall provide round-the-clock streams designated by NASA. At the contract start date these shall include:
- 7.4.2.1 NASA TV Public channel
- 7.4.2.2 NASA TV Media channel
- 7.4.2.3 Audio-only news conferences

7.4.3 Contractor shall deliver capabilities for downloadable audio and video formats compliant with NASA Std 2821 *Audio and Video Standards for Internet Resources*.

7.5 Integration

7.5.1 The Contractor shall work with designated external content partners to provide integrated services such as infrastructure for applications developed by other contractors, website templates developed by content managers

7.5.2 Contractor shall ensure that processes and procedures are established and maintained to support website and web application service coordination and collaboration with NASA and its contractors in the following delivery areas.

7.5.2.1 **Service Delivery Strategy** – Contractor shall assist in developing a strategy that allows multiple contractors to utilize the web services environment.

7.5.2.2 **Service Delivery Responsibility** – Contractor shall assist in developing roles and responsibility guide to share with other service providers who may want to utilize the web services environment. This guidance will include who is responsible for each service delivery task, the location of touch-points or hand-offs, and how their responsibilities change as end-to-end service delivery crosses contract boundaries. Process flows, cross-functional and contract-specific performance work statement elements all play a part in defining roles and responsibilities where coordination is required to ensure continuity of service and operations.

7.5.2.3 **Service Delivery Integration** – Contractor, in accordance with the CF PWS, shall assist in defining the rules of engagement between various parties as well as how to manage the many touch-points and interface requirements between Contractors, end-users, and internal NASA organizational entities.

7.5.2.4 **Service Delivery Performance Assessment** –Contractor shall support service level evaluations, operational or security assessments, financial audits, and other assessments required by the OCIO in response to changing business conditions or governance requirements.

7.5.2.5 **Delivery Communication** – Contractor reporting shall address end-to-end service delivery requirements, ensure the right information is available to the right people at the right time, facilitate operational excellence and support NASA's decision-making requirements.

8 Infrastructure-as-a-Service Requirements

The Contractor shall provide a secure Infrastructure as a Service for storage, backup and recovery, content delivery, platform hosting, service management, and compute.

9 Platform-as-a-Service Requirements

9.1 The Contractor shall provide the platforms required to develop and implement the web applications and websites under the various task orders. These services shall include but not limited to web application development, system integration, Sandbox, database and development/test environments.

10 Software-as-a-Service Requirements

10.1 The contractor shall provide, but not limited to, the following services

10.2 Content Management Tools and Services including:

10.2.1 Content Management System
10.2.2 Wikis
10.2.3 Blogs
10.2.4 Message boards
10.2.5 Moderated Live chats
10.2.6 Syndication

10.3 Collaboration and Social Software Services

10.4 Public and Enterprise Search

10.4.1 The contractor shall work with the NASA enterprise search team to develop an integrated search service

10.5 Analytics and Metrics Reporting

10.5.1 The Contractor shall provide an NASA-wide web-analytics tool for all its public websites.

10.5.1.1 The Contract shall work with the OCIO to determine which analytics will be required.

10.5.2 The Contractor shall provide a web-analytics tool for the internal websites if hosted by the contractor.

10.5.2.1 The Contract shall work with the OCIO to determine which analytics will be required

11 Service Level Agreements

11.1 The contractor shall assist in developing appropriate service level agreements for all services and functionalities identified in this contractor.

Appendices and Reference Documents List

Documents located at http://i3p.nasa.gov/document_file_home.cfm under the WESTPRIME category		
Document	**Document Title**	**Description**
Appendix A	Systems Operated by Current Contractor - Full List	All websites and web applications, both internal and external, hosted and/or managed by current vendor that will require phase-in and transition plan.
Appendix B	Systems Required for RTO 1	All websites and web applications required to be managed under RTO 1.
Appendix C	Descriptive Figures on Web Services at NASA	Figures 1 through 3 that illustrate the Web Offerings, Notional Technology Stacks, and Enterprise Web Services.
Appendix D	Special Event Metrics	Special event metrics, including page views, visitor sessions, hits, and bandwidth peaks. Events included from 2003 to 2012.
Appendix E	Portal Metrics	Portal metrics including visitors, page views, hits, and content. 2004 to present.
Appendix F	Current Operational and Management Capacity	Current capacity of various virtual machine environments.
Appendix G	Service Level Metrics Definition	Service level for availability, performance, security, customer satisfaction, help desk, incidents, and service delivery.
Appendix H	Service Level Methodology	The Service Level Methodology provides description of how SLAs are calculated.
Appendix I	Service Level Performance Matrix	The Service Level Performance Matrix identifies the measurement interval, service level category allocation, expected and minimum service levels.

Documents located at http://i3p.nasa.gov/document_file_home.cfm under the General Documents Category	
Reference Document	**Name of File**
DRD 1294CF-001 through DRD 1294CF-014	I3P Cross Functional DRDS Update_04_12_11 final.pdf
NASA Draft Still and Motion Imagery Metadata Standard	NASA_Image_Metadata_Standard _D6.pdf
NASA Enterprise Service Desk Concept of Operations	ESD_CONOPS_19JAN12_-_signed.pdf
NASA Enterprise Service Desk Performance Work Statement	NASA ESD PWS.pdf
NASA Enterprise Service Management Concept of Operations	NASA Enterprise Service Mgmt CONOPS.pdf
NASA Interim Directive 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements	Replaced by NID 7120.99
NASA Interim Directive 7120.99, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements	NID 7120_99.pdf
NASA Organization Defined Values for NIST SP 800-53 Security Controls and subsequent revisions	NIST SP800-53-rev3-final_updated-errata_05-01-2010.pdf
NASA Policy Directive 1000.0, NASA Strategic Management and Governance Handbook	NPD 1000_0A.pdf

Reference Document	Name of File
NASA Policy Directive 1382.17H, NASA Privacy Policy	NPD 1382_17H.pdf
NASA Policy Directive 1383.1, Release and Management of Audiovisual Products	NPD 1383_1C.pdf
NASA Policy Directive 2810, Information Technology Security	NPD 2810_1D.pdf
NASA Policy Directive 2830.1, EA Policy	NPD 2830_1A.pdf
NASA Policy Directive and NASA Procedural Requirement 1440, Records Management	NPD 1440_6H.pdf
NASA Procedural Requirement 1382.1, NASA Privacy Procedural Requirements	NPR 1382_1.pdf
NASA Procedural Requirement 1441.1, NASA Records Retention Schedules (NRRS)	NPR 1441_1D.pdf
NASA Procedural Requirement 2800.1, Managing Information Technology	NPR 2800_1B.pdf
NASA Procedural Requirement 2810, Information Technology Security	NPR 2810_1A.pdf
NASA Procedural Requirement 2830.1, NASA Enterprise Architecture Procedures	NPR 2830_1.pdf
NASA Procedural Requirement 7150.2, NASA Software Engineering Requirements	NPR 7150_2A.pdf
NASA Standard 2804, Minimum Interoperability Software Suite	NASA Standard 2804-O_FinalSigned.pdf
NASA Standard 2805, Minimum Hardware Configurations	NASA Standard 2805-O_FinalSigned.pdf
NASA Standard 2821, Audio and Video Standards for Internet Resources	NASA-STD-2821BASELINE.pdf
NASA's I3P Cross-Functional Performance Work Statement	CF-PWS - Final Revision2012-06-29.docx

ATTACHMENT B

LOADED LABOR RATES MATRIX

09/07/2012

ATTACHMENT C

ATTACHMENT C – I3P CROSS FUNCTIONAL PWS

CROSS FUNCTIONAL

PERFORMANCE WORK STATEMENT

07/20/2012

Table of Contents

Table of Figures

1. I³P Acquisitions

1.1 Introduction and Overview

To fulfill NASA's requirements for infrastructure improvement the Agency has directed the Office of the CIO (OCIO) to implement a program for providing more reliable and efficient Information Technology (IT) services.

As a result, NASA's OCIO established a major IT improvement initiative in 2007, the IT Infrastructure Integration Program (I³P). Through I³P, the NASA OCIO intends to partner with industry to transform the way IT services are delivered and managed across the Agency.

The I³P strategy includes consolidating service demand across the Agency and working with trusted sourcing partners to deliver standardized, stable, secure, cost effective and high quality IT infrastructure and Enterprise Applications services to the NASA user community.

Specifically, the NASA I³P strategy intends to achieve the following benefits:

a. Enable Agency-wide collaboration through a seamless IT infrastructure;
b. Gain efficiencies in IT infrastructure operating costs;
c. Reduce the complexity of managing IT services across the Agency; and,
d. Improve IT security across the Agency's mission environment.

In addition, the Agency intends to use this improvement initiative to enable a more process-aligned service delivery model across the scope of I³P. This will be accomplished in part by the adoption of the IT Infrastructure Library (ITIL) framework. NASA expects selected IT contractors to demonstrate their capabilities through the application of ITIL processes, specifically ITIL Version 3.0.

As this document is intended to be nearly identical for all I³P contracts, it frequently uses the plural terms "Contractors" and "I3P Contractors." For purposes of this {ACES/NICS/ / EAST/WESTPRIME/Compute Services} contract, the terms "Contractors" and "I3P Contractors," as well as "contractor" shall mean the {ACES/NICS/ EAST/WESTPRIME/Compute Services} Contractor only except where it is patently clear that a specific CF-PWS requirement is a joint responsibility of the I³P contractors (e.g., cooperation, coordination, etc.).

1.2 Concept of Operations

Central to NASA's I³P initiative is the recognition that responsibility for major elements of the Agency's 'As-Is' IT environment, which is currently supported by a variety of independent Agency- and Center-based contracts, will be consolidated into a smaller number of integrated Agency-wide I³P Contracts. Operations and service delivery must remain stable throughout phase-in periods (i.e. transition) to assure that NASA customers do not experience disruption to business operations.

I^3P contractors shall work with the Agency and with each other, in a collaborative and cooperative manner as prescribed by defined processes and assigned roles and responsibilities to transform NASA's fractured IT infrastructure and enterprise applications service delivery capabilities into a highly consolidated, integrated and secure IT Service Management (ITSM) environment.

The OCIO plans to manage this transformation through the I^3P acquisition strategy according to the following four key IT principles:

a. Mission Enabling: IT at NASA serves to achieve NASA's mission;
b. Integrated: NASA will implement IT that enables the integration of business (mission) process and information across organizational boundaries;
c. Efficient: NASA will implement IT to achieve efficiencies and ensure that IT is efficiently implemented; and,
d. Secure: NASA will implement and sustain secure IT solutions.

1.3 I^3P Success Criteria

Successful implementation of the NASA I^3P vision will result in significant benefits to the Agency. Specifically, NASA envisions a "To-be" state characterized by the following criteria:

a. NASA systems can be seamlessly deployed, utilized and secured across Center boundaries;
b. NASA consistently invests in the right IT solutions that provide the greatest benefit to the NASA mission;
c. NASA information is accessible, integrated, and actionable;
d. A reliable, efficient, secure and well-managed IT infrastructure is in place that customers rely on rather than compete with; and,
e. CIOs are seen as credible, trusted partners in solving business problems

1.4 Scope and Boundaries of Contracts

NASA spends approximately $1.8 billion dollars annually on IT. Today, much of the infrastructure supporting NASA is decentralized including operations at NASA Headquarters, all ten NASA field Centers, and associated component locations. There are major challenges in IT management associated with a decentralized IT organization, such as lack of sufficient visibility into IT spending, inability to achieve economies of scale, inconsistent IT governance and numerous information security challenges.

NASA is consolidating IT service demand, transforming service delivery, aligning IT management and enhancing IT security through I^3P. The acquisitions making up I^3P include the following enterprise services:

a. ACES (Agency Consolidated End-user Services): End-User Services –includes NASA desktops, cell phones, Personal Digital Assistants (PDAs), a portion f NASA's Identity, Credential, and Access Management (ICAM) services including NASA's Consolidated Active Directory (NCAD) and issuance of Agency logical credentials, e-mail and calendaring functionality;
b. NICS (NASA Integrated Communications Services): Communications Services – includes data, voice, video, Local Area Network (LAN) and Wide Area Network (WAN) services;
c. Compute Services –includes application/data hosting and housing;
d. WESTPRIME (Web Enterprise Service Technologies): Web Services – to include public-facing website hosting and applications; and,
e. EAST (Enterprise Applications Service Technologies): Enterprise Applications Services –includes applications services associated with the NASA Enterprise Applications Competency Center, a portion of NASA's ICAM services including authentication services and the NASA Access Management System (NAMS), Agency-wide collaboration services, and new intranet environments and applications.

Today, these services are provided under Agency-wide service contracts and additional Center IT Infrastructure contracts. The existing contracts are identified in the Tables below.

Location	Contract Name	Contract Number	Contractor
HQ/OCIO	NASA Web Portal Services	GS-35F-0627P	eTouch
MSFC	Enterprise Application Service Technologies (EAST)	NNM04AA02C	SAIC
MSFC	Agency Consolidated End-user Services (ACES)	NNX11AA01C	HP Enterprise Services
MSFC	NASA Integrated Communications Servcies (NICS)	NNM11AA04C	SAIC
NSSC	Enterprise Service Desk (ESD)	NNX05AA01C	CSC

Table 1: Current Agency-wide Contracts

Location	Contract Name	Contract Number	Contractor
ARC	Ames-Consolidated IT Services Task Order 2 (ACITS2)	NNA08AF13C	Dell Federal Government Services (DFGS)
DFRC	Research Facilities and Engineering Support Services (RF&ESS)	NAS4-00047	Arcata Assoc.
GRC	Professional, Administrative, Computational and Engineering Support Services (PACE III)	NNC08BA09B	DB Consulting Group, Inc
GSFC	Goddard Unified Enterprise Services and Technology (GUEST)	NNG10FE01C	ASRC Primus

HQ	Headquarters Information Technology Support Services (HITSS)	NNH12CF39C	Digital Management, Inc. (DMI)
JSC	JSC Information Technology and Multimedia Services (ITAMS)	NNJ11JA16B	DB Consulting
KSC	Information Management and Communication Support (IMCS)	NNK08OH01C	Abacus Technology
LaRC	Langly Information Technology Enhanced Services (LITES)	L70750D	Stinger Ghaffarian Technologies (SGT)
MSFC	MSFC IT Services (MITS)	NNM10AA03C	Dynetics
NSSC	NASA Shared Services Center (NSSC)	NNX11AA02C	CSC
SSC	Information Technology Services (ITS)	NNS04AB54T	CSC

Table 2: Current Center IT Infrastructure Contracts (Partial List)

The figure below represents how the remaining services under current Agency-wide and Center IT infrastructure and support services contracts map into the I^{3}P acquisitions. The diagram is intended to represent the concept only and not specific contract scope decisions which are specified within each of the individual contracts.

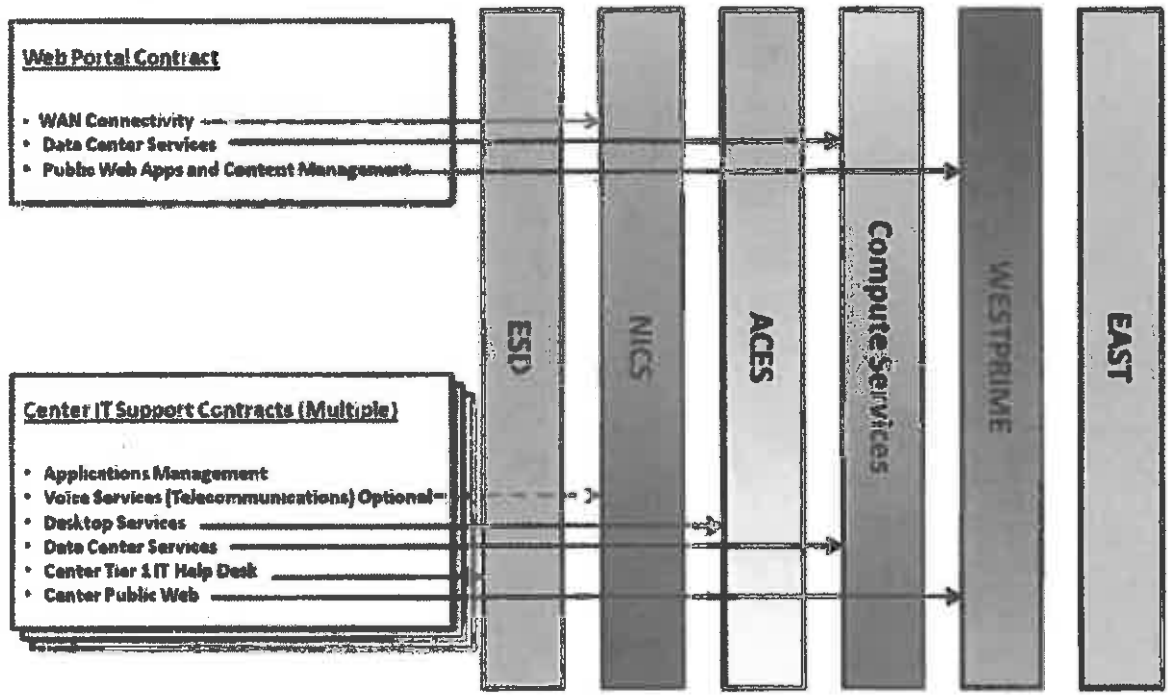

Figure 1: Concept of mapping current Agency and Center contracts to I^{3}P contracts

Compute Services are not managed through a single Agency-wide contract, but rather through a series of existing and planned contract vehicles:

In response to the Federal Data Center Consolidation Initiative (FDCCI), NASA is reducing the overall number of data centers and focusing on "regional" consolidation, ensuring suitable data center capabilities exist at each major NASA facility. The Federal initiative imposes a moratorium on the creation or acquisition (leasing) of any new data centers. Contractors needing access to data centers to house or host NASA or Center systems, storage or data should contact the CIO at the affected or closest center to discuss the requirements and make arrangements for using an approved NASA data center.

In alignment with the FDCCI, NASA is prohibiting the creation of new "server rooms" and "server closets", where office or other non-data center space is reallocated to house small numbers of servers and/or storage without CIO approval. NASA is in the process of consolidating the contents of all existing "server rooms" and "server closets" into approved data centers. Anyone considering creating a new "server room" or "server closet" should immediately contact the appropriate Center CIO to identify the approved data center that can accept the assets in question.

Consistent with the FDCCI and also in compliance with the 25 Point Plan for IT Reform, NASA is actively addressing the adoption of cloud computing. The NASA Office of the CIO is pursuing an enterprise cloud service offering for commercial cloud services that will allow NASA to aggregate cloud purchases to receive volume pricing and to implement compliance to IT security requirements with least impact to the end users. Anyone needing or considering the use of cloud computing services should contact the affected Center CIO or the OCIO Computing Services Service Office to discuss existing available options.

1.5 Client Facing and Support Services Contracts

ITIL defines client facing services as services that are delivered to end-users of the business (e.g., email, billing, etc.). Support services are defined as services necessary to support the operation of the delivered service (e.g., data center services, managed network service, etc.).

The relationship between Client Facing (Core) Services and Supporting Services is depicted in diagram below.

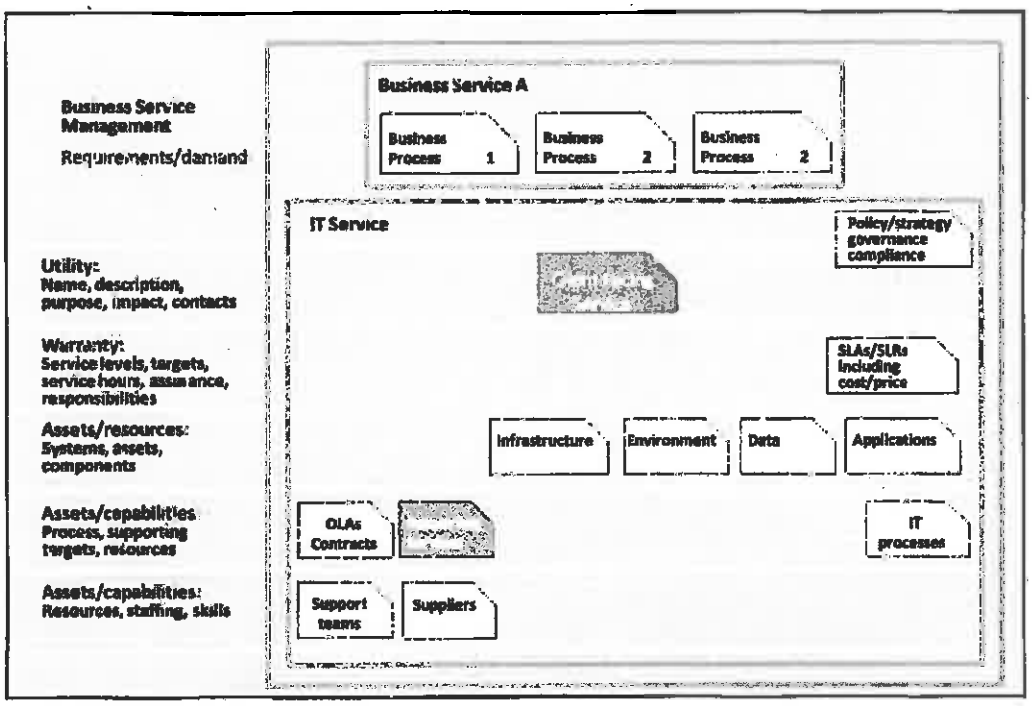

Figure 2: Relationship between client facing and supporting services

All I^3P contracts will provide some level of client-facing service delivery. For the purposes of general discussion, NASA's I^3P contracts are classified as client facing or support service contracts based on a significant majority of requirements being either client or support services as follows:

a. Client Facing Contracts:
   1. ACES – End-user services
   2. EAST – Enterprise application services
   3. WESTPRIME – Web services

b. Support Service Contracts:
   1. NICS – Communication services
   2. Compute Services (multiple contract vehicles expected)

1.6 Cross Functional and Collaboration Activities

Each of the contracts includes a Performance Work Statement (PWS) consisting of defined work activities and Contractor requirements specific to each of NASA's independent service contracts. These PWS's also define roles and responsibilities for the Contractor as they relate to NASA's requirements.

In addition to service-specific performance work statements, there are a number of contractor work activities and responsibilities that cut across all I^{3}P contracts. These Cross-Functional Performance Work Statement (CF-PWS) requirements, contained in this document, are common to each of the contracts. The CF-PWS defines NASA's requirements for synchronization of effort and solution integration across NASA and multiple contracts supporting the I^{3}P initiative. NASA has taken every effort to ensure that there are no conflicts between the CF-PWS and the contract-specific PWS. If any conflicts do exist, the CF-PWS will take precedence.

Consistent application of these cross functional requirements is central to NASA's desire to standardize processes using the ITIL Version 3.0 framework and is essential to an effective, integrated enterprise service delivery.

1.7 Service Level Agreements

Service Level Agreements (SLAs) are an important aspect of NASA's service-based organization and the I^{3}P contracts. An SLA specifies the level, scope and quality of a service that will be provisioned, from the business customers' perspective. The SLA clarifies how the service provision will be measured, and the penalty to be exacted if the service is not delivered to the agreed level of service.

Service delivery under the NASA I^{3}P program will require the involvement of multiple providers to meet the SLAs established by the NASA business customer. Providers shall work together in the best interest of NASA as described in Section 3. The diagram below depicts how an SLA will be segmented into independent Contractor service levels. Contractor-specific service levels are specified in each of the I^{3}P contracts.

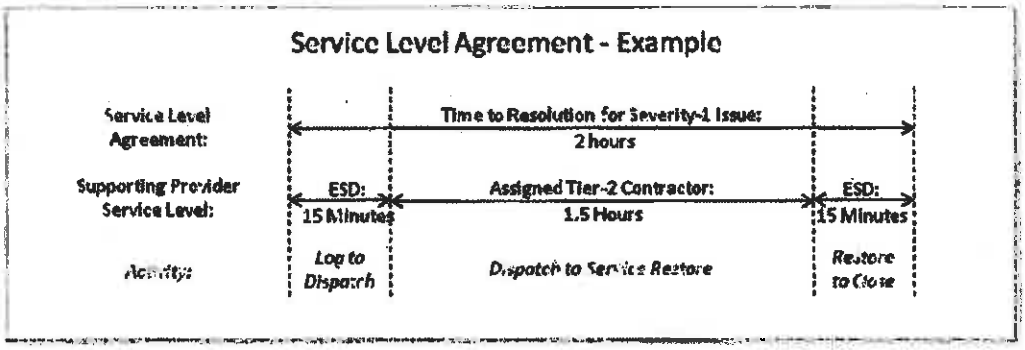

Figure 3: SLA Integration Concept

In the example diagram above, the SLA for restoration of service to the customer for a Severity 1 issue is two hours. The Enterprise Service Desk (ESD) would have a maximum time of fifteen minutes to escalate the call to the appropriate Tier 2 contractor. At that point, as specified in the Tier-2 contractor SLA, the Tier 2 contractor would have a maximum of one and a half (1.5) hours to correct the problem and restore service before assigning the incident back to the ESD

for call closure. After Tier 2 has reassigned the incident to the ESD, the ESD would again have a maximum of fifteen (15) minutes to verify service restoration with the customer and close the call. The sum of the ESD and Tier 2 contractor SLAs (15 minutes + 1.5 hours + 15 minutes) would equal the customer Service Level (2 hours). In this example, only one Tier 2 contractor is involved with the service restoration, but in some cases multiple Tier 2 providers may be involved. I^3P Enterprise Service Management (ESM) leadership will coordinate service restoration efforts that span multiple providers. In all cases, Tier 2 providers are accountable only for the service level agreements specified within their individual contract.

2 IT Service Management: Organization and Governance within NASA

2.1 Introduction and Overview

NASA is transforming the Agency's IT infrastructure and applications services environment through I³P. This transformation requires changes in the way NASA manages IT across the Agency including the need to define and clarify roles and responsibilities within the NASA IT organization to assure success of the I³P initiative.

As with most organizations, the NASA IT organization is continually changing and maturing to better meet the evolving needs of the customer base it serves. This section outlines the roles and responsibilities across the IT organization within NASA. Two new elements are defined to support the transformation that is underway, including the establishment of ESM functions within the Agency CIO organization and the creation of Service Integration Management (SIM) within the Agency CIO's Enterprise Service & Integration Division (ES&ID). Contractors providing IT services to NASA shall establish appropriate roles and responsibilities in support of NASA's ITSM vision as described in this section.

2.2 The NASA IT Organization: Roles and Responsibilities

The NASA CIO established I³P and is responsible for overall direction and leadership of the program, within the larger context of NASA's IT organization. Before discussing the NASA IT Organization, it is important to understand the charter and purpose of I³P:

> **I³P Charter:** Provide a NASA Enterprise service support environment that optimizes the ITIL best practice processes for implementing formal ITSM.
>
> **I³P Purpose:** The I³P initiative seeks to standardize NASA's ITSM practices, align with industry best practices (e.g., ITIL), and yield a set of consistent, repeatable and measurable processes for service delivery to NASA OCIO customers.

The NASA IT organization is comprised of multiple elements serving Agency, Mission, and Center customers and organizations. The elements of the NASA IT organization are defined below, including an overview of the roles and responsibilities of each part of the organization.

2.2.1 Agency CIO

The NASA CIO is accountable for all aspects of IT within NASA as well as for the overall leadership of the NASA IT organization including the establishment of strategy, enterprise architecture, and operational policies and standards to support the NASA mission. To accomplish these functions, the NASA Office of the CIO is organized into 4 divisions including ES&I, IT Security, and Capital Planning and Governance, and the Chief Technology Office (CTO). Within this structure the NASA CIO has also established functions associated with Enterprise Architecture (EA), Systems Engineering and Integration (SE&I), Service Executives

(SEs), and SIM. Through integration with the SIM, the ESD provides critical integration functions in support of Agency ESM. Finally, the NASA CIO is also accountable for establishing a NASA governance model that effectively interconnects the various components of the Agency-wide IT organization and enables effective decision making at all levels within that organization. This governance spans not only the elements of the Agency CIO's office, but also Center and Mission Directorate CIO organizations; these will be described later in this document.

2.2.2 Enterprise Service Management

To support effective delivery of enterprise IT services, the ESM function is performed by ES&ID, interfacing with the other Agency CIO Divisions. ESM provides a NASA Enterprise service support environment that optimizes ITIL best practice processes for implementing formal ITSM. The purpose of ESM within NASA is to standardize NASA's ITSM practices, to align with industry best practices, and to yield a set of consistent, repeatable, and measureable processes for service delivery to NASA OCIO customers. Within the NASA IT structure, ES&ID accountable for:

a. Service Strategy direction on how to design, develop and implement ITSM.
b. Service Design direction for the design and development of IT services and ITSM processes.
c. Service Operations direction on achieving effectiveness and efficiency in the delivery and support of IT services so as to ensure value for the customer and the IT service providers, including effective coordination across all service providers.
d. Continuous Service Improvement direction in creating and maintaining value for customers through better design, transition and operation of services.

Within the NASA Office of the CIO, ES&ID is responsible for overseeing EA, SE&I, SEs, SIM, and coordination with the various I^3P service offices. Each of these areas will now be further described briefly, with additional detail available in the NASA ESM Concept of Operations document.

2.2.3 Enterprise Architecture (EA)

The OCIO Enterprise Architecture Office is responsible for articulating the mission supporting technologies and operational model to accomplish the IT goals. The EA Office develops baseline architecture and target architecture and their associated sequencing. The EA Office therefore, has responsibility for ensuring that the current-state service catalog evolves to meet future customers' expectations. As part of Service Strategy, the EA Office must work in concert with the center CIOs, SIM, and SEs to ensure that customers' requests and opportunities for service improvement are effectively addressed in its service strategy efforts.

All I^3P service architectures will be developed and maintained by NASA enterprise, mission and service domain architects in partnership with the I^3P Contractors. These architectures shall

follow enterprise or segment architectural policy, guidance, and standards defined by NASA[1] or the Office of Management and Budget[2] to achieve NASA's strategic IT target state goals as stated in the NASA Information Resources Management (IRM) Strategic Plan. The outcome of this approach will ensure that IT investments are aligned with NASA's vision for the future and that technology solutions are horizontally integrated across business domains.

In order to achieve viable service architectures, it is imperative that NASA and the I^3P contractors collaborate on the analysis of emerging technologies, NASA requirements, and the as-is environment. The result of this collaboration shall be an innovative to-be state, identification of gaps between the as-is and to-be states, and a transition strategy for each service area that will position NASA and the I^3P contractors for success.

Each service architecture shall address the service, systems and components (see Figure 4) required to provide the specific service and ensure integration with the other service architectures and the NASA enterprise architecture.

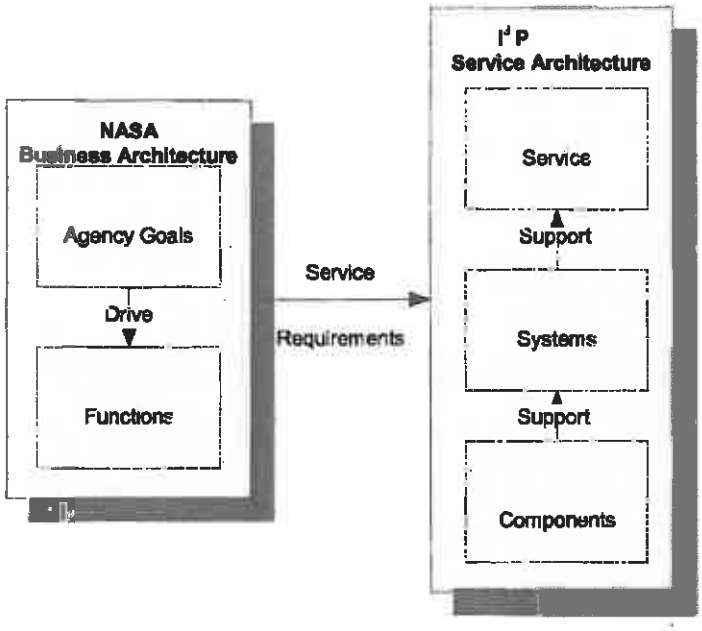

Figure 4: NASA Business and Service Architectures

2.2.4 Systems Engineering and Integration (SE&I)

The OCIO ES&ID organization's SE&I component is accountable for the design of new services including the development of cost estimates associated with these new offerings. The SE&I

---

[1] Examples include NASA NDP/NPR 2830.1 EA Policy, NASA-STD-2804 Minimum Interoperability Software Suite, and NASA-STD-2805 Minimum Hardware Configurations.

[2] Examples include the Federal Enterprise Architecture Framework (FEAF), FEA Core, Business Service, and Enterprise Service Segments, and the Practical Guide to Federal Service Oriented Architecture (PGFSOA) v1.1

group also ensures that new and existing services are translated into the NASA technical reference model (TRM) and that all changes to the NASA enterprise IT environment are managed through the appropriate change advisory boards (CABs). These engineering and integration functions also include the establishment of service configuration and performance expectations, reflected in appropriate performance definitions, service metrics and evaluation criteria. Under the ESM concept, the SE&I group is responsible for risk assessments and impact analyses associated with the delivery of existing and new enterprise services. Finally, the SE&I group is responsible for the coordinated deployment of new and updated services.

2.2.5 Service Executives (SEs)

Service Executives are the actual service owners for the respective I^3P services for which they have responsibility. In this role as service owners, the SEs are accountable for the configuration of services and the vetting of these services through the appropriate change advisory and control boards within the Agency. SE's are responsible for the development of their specific service strategies and the budgetary requirements to implement these strategies if approved. In order to effectively carry out their responsibilities, each SE must actively engage the NASA user community. This customer relationship management function is essential in identifying issues and gaps in current service delivery to support the development of strategies that will enable continuous service improvement.

Each SE also handles contract performance escalation management in those situations where an issue cannot be resolved at the service office level, or when an issue may span multiple enterprise services and resolution requires coordination at the ESM level. In addition, managing particularly high-impact service issues that impact day-to-day performance will also be escalated to the SE for communication and possible action. Finally, the SE is responsible for collaborating with the service office(s) responsible for the day-to-day management of service delivery to define Service Office Manager (SOM) objectives and milestones.

2.2.6 Service Integration Management (SIM)

The Service Integration Manager is responsible for process architecture and design leading to the implementation of ITIL best practices across the enterprise. The SIM will provide support for designing and implementing the NASA ITIL processes and instituting formal ITSM within NASA. The purpose of the SIM is to improve the effectiveness and efficiency of NASA IT operations through the design, implementation, and operations of standardized ITSM practices. Primary functions of the SIM include:

a. Support strategic planning associated with defining and scoping the future ITIL-aligned Service organization.
b. Direct and coordinate implementation of the strategic plan.
c. Provide Continuous Service Improvement and ITIL process management for NASA's IT organization.

The SIM will also provide ESD oversight and integration, along with the integration of performance metrics across all enterprise services. These metrics provided through ESD systems, Contractor deliverables, and customer surveys will be used by the SIM to obtain a 'big-picture' view of service performance, leading to service improvement recommendations. Additional information about the ESD is provided in the following section.

2.2.7 Enterprise Service Desk

The mission of the ESD is to be the Single Point of Contact (SPOC) for Enterprise Services support, handling incidents and requests, and providing an interface for activities such as changes, problems, configuration, releases, service levels and IT Service Continuity Management. The importance of the ESD as a SPOC is to provide a consistent interface to the end-user community, which is a critical element of the business' determination of how well NASA IT is performing its job – one of the success criteria of the I^3P program.

The primary priorities of the ESD are:

a. To manage customer expectations by identifying and communicating I^3P services to customers. Route customers to the appropriate point of contact for those services not provided directly by the ESD or an I^3P service provider.
b. To return the customer to normal operations within SLA requirements and specifications.
c. To continuously improve service performance.
d. To perform consistent workflow, enabling service request escalations across disparate IT infrastructure contracts.
e. To provide reliable communications coordination for Enterprise Service outages.
f. To collect, consolidate, analyze, and report performance metrics across the independent IT service providers for Enterprise Services provided to customers.
g. To provide the SIM with accurate and appropriate data that enables responsible operational decisions.
h. To leverage existing NASA infrastructure to reduce costs.
i. To provide integrated service support interfacing to functional areas of Procurement, Finance and Human Resources.

2.2.8 Service Offices

Located at each of the sites hosting an I^3P service contract, Service Offices are accountable for the day-to-day management and delivery of the enterprise services that they manage. Service Offices are expected to coordinate across SOMs, Contracting Officer's Technical Representatives (COTRs) and Contracting Officers (COs) to ensure the effective delivery of services across the Agency. While these offices are physically located at and managed by specific Centers, they perform an Agency function.

The Service Offices are also responsible for the management and synthesis of I^3P contract service performance and financial information, and communication of this information through the SIM and the appropriate SE. In terms of communication, the Service Office provides information to the Agency CIO, SEs, Center Subject Matter Experts (SMEs), SIM, and to the Center and Mission Directorate CIOs to ensure that all levels of the NASA organization remain informed regarding important performance or service delivery issues.

Service Offices manage the day-to-day financial transactions and issues associated with the services they manage, and will escalate complex contract and performance issues as required. Service Offices will work closely with the I^3P service providers to manage technical issues as well as to ensure that contractual service levels are consistently being achieved.

SOMs are responsible for each specific IT service contract under the I^3P services umbrella. They are the coordinator and Point of Contact (POC) for a specific service offering e.g. LAN services as opposed to WAN services. They are accountable for adherence to the day-to-day operational parameters for performance of the service as defined in the SLAs, and facilitate service operation activities. The SOM performs oversight of service supplier activities (contractor oversight) and communicates IT service performance issues to the SE. They provide customer relationship management support to the CIOs relative to Enterprise (Agency) services.

In order to provide a coordinated and consolidated technical picture of the individual I^3P contracts, each Service Office will designate an Integration Lead (SOIL). The SOIL supports the SE and SIM offices ensuring contracted service providers across the Centers are working in accordance with (and to established) Agency standards, regulations, processes and procedures. SOILs work with peer SOILs and Center Integration Leads (CILs) to ensure integration across contracts for projects and processes and support service performance monitoring and reporting to SOMs, SEs and SIM in regards to individual contracts.

2.2.9 Center CIO

With the implementation of I^3P and the resulting shift from local to enterprise delivery of some services, the role of the Center CIO and the staff they manage is evolving. As the roles and responsibilities shift to support the NASA IT strategy, the Center CIOs maintain significant responsibility for local service delivery, and have acquired new roles associated with enterprise service strategy and delivery. These roles and responsibilities are described in the following section.

Relative to local service delivery, Center CIOs are accountable for the day-to-day delivery of locally-provided IT services that are not provisioned as part of one of the Agency service contracts. This includes all aspects of managing these services including service design, implementation, monitoring, security, and continuous improvement. The Center CIO is also accountable for ensuring that any locally-provided services align with Agency strategy and policy. Center CIOs ensure the provisioning of local infrastructure to enable effective and efficient delivery of enterprise services while overseeing the Center's overall IT portfolio and managing demand for both local and enterprise services. The CIO is ultimately responsible for

customer relationship management across all organizations at the Center, and ensures that requirements, issues, and concerns regarding IT services are captured, understood, and addressed. In terms of strategic leadership, each CIO is a member of the Center's executive leadership team responsible for solving business problems through the application of innovative IT solutions. In a similar manner, each Center CIO is a member of the Agency IT Management Board (ITMB) and is responsible for setting the Agency's strategic direction relative to information and information technology.

Center CIOs also have significant responsibility relative to enterprise service delivery. Because the Agency has such a highly-skilled IT workforce spread across all Centers, each CIO will identify SMEs to support each of the enterprise services at their respective Center. In addition to these SMEs, a CIL will be identified to coordinate and manage issues involving integration across multiple services. These SMEs and CILs will work closely with the associated SEs, Service Offices and the SIM to effectively implement enterprise delivery of key services. As additional requirements are identified for new or improved services, Centers CIOs will also identify and provide technical experts to participate on Agency-level technical and architectural teams. Finally, the CIO will serve as the voice of the Center customers to Agency service providers while monitoring service integration and performance issues locally and participating in continuous service improvement efforts.

Those CIOs whose Centers host Service Offices have additional responsibilities including working with the Agency CIO to determine the resources required to manage and execute the project as agreed to with the Agency OCIO. Host Center CIOs also work with the appropriate SE(s) to define performance objectives for local staff members who are supporting enterprise service delivery and then manage the service office staff to ensure that the Center delivers on these Agency commitments.

2.2.10 Mission Directorate CIOs

Similar to Center CIOs, Mission Directorate CIOs represent the requirements of their respective missions, which cut across all NASA Centers. The Mission Directorate CIO has a unique understanding of the mission requirements related to information and information technology and works with Center and Agency IT Service providers to ensure that these requirements are satisfied. Each Mission Directorate CIO is a member of the ITMB and is responsible for helping to set the Agency's IT strategic direction and provides a critical customer relationship management function as the voice of the mission customer regarding all aspects of NASA IT services.

2.3 NASA IT Governance Process and Structure

Contractors shall adhere to the NASA OCIO governance strategy and framework as outlined in this section and discussed in greater detail within each respective I³P contract and associated performance work statements.

In conformance with NASA's IT governance process, contractors shall:

a. Support NASA's Mission via ongoing alignment and management of NASA's IT assets and processes with its mission requirements and strategic initiatives.
b. Identify potential areas of investment redundancy and opportunities for consolidation, rationalization and cost efficiency.
c. Support master planning at the Agency level to increase visibility of and better prioritize investments.

NASA's approach to IT governance is a structured, decision-oriented model that has critical linkages to NPR 7120.7 NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements and other NASA IT management processes such as capital planning and investment, IT security planning, and EA as defined in various IT-related policy documents (NPR 2800.1, Managing Information Technology, NPR 2810.1 Security of Information Technology, and NPR 2830.1 NASA Enterprise Architecture Procedures).

NASA's IT environment is organized into three major areas, or portfolios:

a. IT infrastructure services
b. IT applications
c. Highly-specialized IT, such as technology that supports real time control systems and on-board avionics

While some cross-cutting IT processes, such as IT security, apply to all portfolios, the scope of IT governance described in this section applies primarily to IT infrastructure and application services.

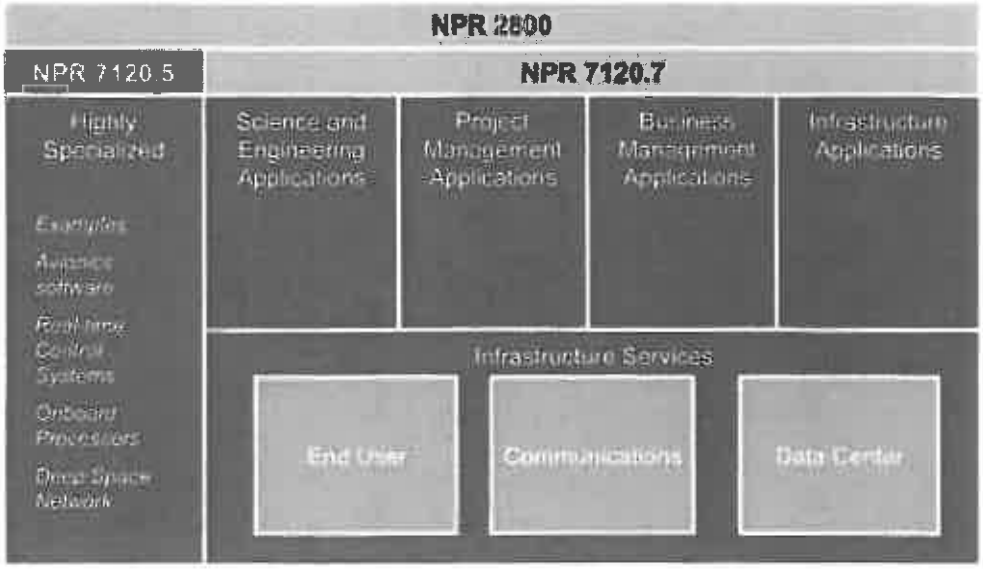

Figure 5: IT Portfolios and Governing Policies

To address the wide-ranging decisions which are likely to occur throughout the life cycle of the I³P contracts, at an Agency level NASA employs a board model where each board has a clear set of responsibilities as well as interfaces to the other governing bodies. This governance model shown below provides complete coverage of the life cycle of an IT investment from the initial decision to fund a proposed investment to the oversight of its implementation and operations and subsequent decommissioning. Each of these life cycle phases has associated with it unique milestones and metrics that require different activities and therefore different board oversight.

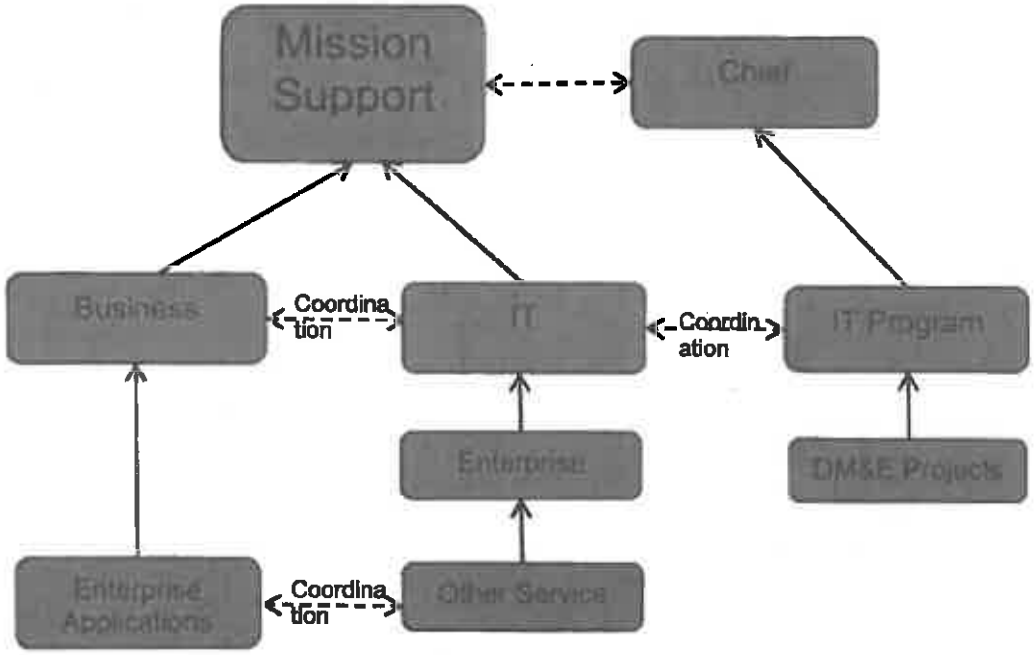

Figure 6: NASA IT Governance Structure

The scope and purview of each NASA board is further defined as follows:

a. **Mission Support Council (MSC)** – Decisions regarding NASA strategy and related investments (prioritization and selection), and NASA-wide policies/processes. Members include senior executives from Mission Directorates, Mission Support Offices, and Centers.

b. **Business Systems Management Board (BSMB)** – Decisions regarding strategy and related investments for the Agency Business Systems portfolio. Members include senior level stakeholders from the functional business areas.

c. **IT Management Board (ITMB)** – Decisions regarding strategy and related investments for the I3P portfolio of services. Decisions regarding operational performance and issues related to performance. Members include the Agency OCIO Division Directors, Center and Mission Directorate CIOs.

d. **IT Project Management Board (IT PMB)** – Decisions regarding application and infrastructure projects to ensure that investments approved by the ITMB, BSMB, or

MSC stay on track during formulation, design and implementation. Members include the Deputy CIO,, Enterprise Architect, and representatives from Mission Directorates, Mission Support and Centers.

e. **Enterprise Change Advisory Board (E-CAB)** – Decisions regarding technical integration and service integration across Service areas. Members include the Technical Integration Manager, Service Integration Manager, CTO, Enterprise Architect, and Service Executives.

The governance structure described above operates at the Agency level and addresses major IT investments that cross Center and program boundaries.

NASA's approach to IT governance reflects the latest in industry best practices and is grounded in the strategic management principles for governing, managing, implementing, monitoring, and controlling the work of the Agency as set forth in the Strategic Management and Governance Handbook, NPD 1000.0.

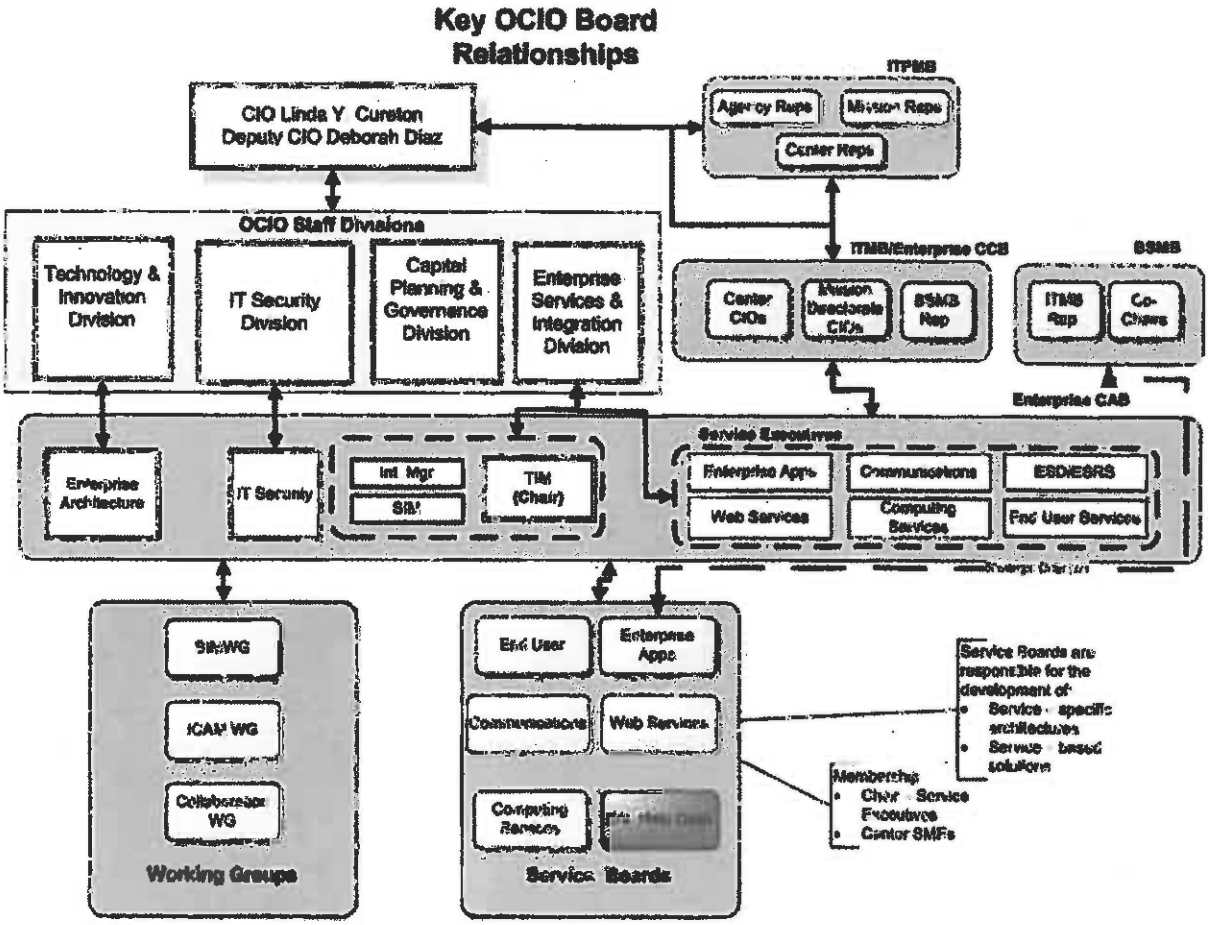

Figure 7: I3P Governance Structure

The I3P governance structure is depicted in Figure 7. Each service area has a Service Board, which is authorized to make decisions within the scope of the service. Decisions that impact multiple service areas, have a high level of risk, and/or high visibility to customers and stakeholders, are made at the E-CAB and ITMB level.

Each Service Board may have one or more working groups which are established to provide analysis and recommendations within their scope to the cognizant Service Board. Working Groups are formally chartered and approved by the E-CAB and ITMB. Communities of interest may also be established to foster the exchange of ideas. Communities of interest have no formal decisional authority. While no formal approval is required for a Community of Interest to be established, a Board or Working Group may sponsor a Community of Interest.

Centers are also implementing local governance structures that, while customized to the unique organizational environment and culture at each Center, conform in spirit to the I^3P governance structure and enable Center-specific investments to be addressed. Notwithstanding the existence of Agency or Center-specific governance structures, it is expected that changes will need to be made over the life of the I^3P Acquisition to address the full IT life cycle as described in NPR 7120.7.

2.4 Contractor Responsibilities

In addition to working with NASA in concert with Agency level governance processes and structures, contractors must work within other complementary contract and relationship management mechanisms as defined within each contract.

These additional governance processes and structures relate to the Contract administration and management activities that are specific to the individual NASA Centers responsible for procuring and overseeing delivery and performance as defined in the individual I^3P performance work statements. Contractors should refer to the individual contracts for details of these complementary governance processes and structures.

The I^3P contractors shall work closely with the ESM and SIM organizations to ensure adherence to NASA standard IT processes, monitor compliance, drive continuous service improvement and coordinate service operations to achieve an effective and efficient multi-sourced IT environment in support of Agency requirements. I^3P contractors shall work closely with Center CIOs to understand requirements and to work local service delivery issues.

While specific requirements are captured in the cross-functional ITIL process requirements, an overview of these responsibilities associated with supporting ESM and SIM activities is provided below.

a. **Policies and Procedures:** Contractors shall support SIM identification, definition and implementation of changes to Agency IT policies and procedures that improve service delivery, streamline operations and reduce costs. Contractors shall do this

through the identification and application of Industry best practices, methodologies and tools within the NASA ITSM environment.

b. **Strategy Development:** Contractors shall participate in the Agency's annual portfolio management process by providing design, cost, benefit, risk and other information necessary for the ESM to prioritize a list of projects aligned with user requirements.

c. **Process Development:** Contractors shall support service integration by defining and implementing service delivery processes and procedures identified in the Agency's Cross Functional Statement of Work and other contractor processes that are complementary to NASA's ITIL v3 aligned processes.

d. **Process Interface:** Contractors shall ensure that cross-contract service integration and delivery touch-points are aligned with both Government and other I³P contractors so that seamless service delivery and management occurs.

e. **Compliance Monitoring:** Contractors shall support the Agency in monitoring of service delivery to the end customer. Such monitoring shall include, but not necessarily be limited to, process quality assurance, escalating and resolving issues (inclusive of cross-contract/vendor), monitoring production control, and integrating actions, communications and exchanges of service supporting data activities across I³P contractors to ensure customer support requirements are met (i.e. SLAs are met).

f. **Operations Coordination:** Contractors shall support NASA's management of the multi-sourcing environment by supporting coordination and oversight of operations.

g. **Continuous Service Improvement:** Contractors shall identify, define and implement continuous service improvement activities. Contractors shall benchmark projects as defined by SIM's continuous improvement processes.

2.5 Relationship Management

Contractors shall follow a robust Governance model to partner with NASA and manage both services delivery and contract performance. Relationship management focuses on actively managing relationships with NASA customers, stakeholders and other contractors who are integral to the delivery of integrated ITSM under I³P. All relationship management practices are ongoing and entail the following set of activities:

a. Managing interactions with NASA to ensure their effectiveness and to capture critical service level information.
b. Formally managing relationships with NASA customers and contractors by establishing relationship objectives and tracking performance of those objectives.

c. Selecting suppliers and partners based on their ability to meet NASA business requirements.
d. Obtaining feedback from NASA stakeholders, including employees, and contractors on the nature and quality of key service and delivery relationships.
e. Proactively identifying opportunities that will provide additional value to NASA.

The NASA IT governance structure is designed to encourage collaborative discussion of issues and ideas critical to the ongoing success of I³P and related IT transformation. As detailed in the individual I³P contracts, each party shall designate an individual to serve as a relationship manager who will be that party's SPOC for all matters relating to the outsourcing contract. The contractor's relationship manager shall:

a. Be knowledgeable about NASA's I³P service requirements and each of the contractor's and its subcontractors/partners products and services.
b. Be experienced at running IT systems and networks, as they relate to the provision of services for which they are contracted, of similar size to NASA's current and anticipated business requirements.
c. Have overall responsibility for directing all of the contractor's activities.
d. Be assigned to the NASA account for a significant portion of the contract term.

Contractors shall assist and contribute to setting the strategy and processes concerning NASA's technology and use over the life of each I³P contract. Contractors shall continually evaluate the technical environment, identifying potential enhancements that will reduce overall costs while delivering high quality and high availability services across the Agency.

3 Service Coordination and Collaboration

3.1 Introduction and Overview

The I³P acquisitions involve more than management of independent sourcing agreements. The effort will require coordination, collaboration and integrated management of key processes among contractors and across contract boundaries.

It is in the coordination of multiple contractors where the management of I³P services differs from the management of independent IT contracts. Coordination of services across these multiple contracts involves coordinated management of four sets of relationships:

a. Between NASA end users and individual Contractors;
b. Between NASA leadership and individual Contractors;
c. Between NASA's internal client facing and support organizations required to deliver IT services; and,
d. Between the I³P Contractors.

It is important that contractors work with NASA and with each other to establish and execute common management approaches and procedures to ensure that services are provided effectively and efficiently across the enterprise regardless of contractual boundaries.

3.2 Service Delivery Coordination and Collaboration

NASA recognizes the interdependencies of internal and external relationships and expects contractors to work with the Agency and among themselves to proactively manage those interdependencies to support the overall mission, vision, and objectives of the OCIO.

Contractors shall ensure that processes and procedures are established and maintained to support service coordination and collaboration with NASA and other I³P contractors in the following delivery areas.

a. **Service Delivery Strategy** – Proactive management of NASA's service delivery strategy assumes that business conditions and customer requirements change over time requiring that initial strategies adapt to changes as they occur. By working with NASA to modify goals, priorities, policies and procedures as they affect one or more of the sourcing relationships, I³P Contractors shall continuously improve how services are delivered to meet end user needs.

b. **Service Delivery Responsibility** – Management of service delivery can be complex when multiple contractors are responsible for IT service delivery. I³P contractors shall know and understand who is responsible for each service delivery task, where touch-points or hand-offs are and how their responsibilities change as end-to-end service delivery crosses contract boundaries. Process flows, cross-functional and

contract-specific performance work statement elements all play a part in defining roles and responsibilities where coordination is required to ensure continuity of service and operations.

c. **Service Delivery Integration** – Coordination and collaboration across multiple contractors demands that multiple contractors work together and, as needed, shall co-develop processes that define the rules of engagement between various parties as well as how to manage the many touch-points and interface requirements between Contractors, end-users, and internal NASA organizational entities. Proactive management of delivery integration not only ensures that everything that needs to get done is accomplished, but that contractors work together to identify, create and document any new procedures necessary to ensure seamless service delivery to NASA customers over time.

d. **Service Delivery Performance Assessment** – Proactive management of service performance processes are focused on verifying the facts of the relationship through coordination and cooperation among NASA I^3P and other supporting Contractors. The contractor shall support service level evaluations, operational or security assessments, financial audits, and other assessments required by the OCIO in response to changing business conditions or governance requirements.

e. **Delivery Communication** – Proactive management of communications and feedback requires the transmission of information generated throughout service creation and service delivery processes. Contractor reporting shall address end-to-end service delivery requirements, ensure the right information is available to the right people at the right time, facilitate operational excellence and support NASA's decision making requirements.

NASA's ESM will be the focal point to ensure seamless IT service delivery.

4 NASA IT Infrastructure Library (ITIL) Version 3 Approach

4.1 Introduction and Overview

In support of the Agency CIO's vision for I^3P, various IT operational models were analyzed and the ITIL version 3.0 framework was selected. Applicable ITIL v3 processes have been identified and prioritized for development and implementation within the NASA IT environment. It is recognized by the NASA ITMB that a common and consistent Agency-wide IT organizational management structure is required to support centralized, Agency-provided IT services. The new ITIL processes will be designed to enable and support IT governance via performance metrics. The adoption of a standardized framework that includes a common terminology and process set will be an integral part of all I^3P support contracts. ITIL version 3.0 focuses on Service Management and seeks to align IT with business objectives. ITIL version 3.0 outlines a set of integrated processes that encompass the full scope of the IT service lifecycle. By defining a common set of ITIL version 3.0-aligned processes that are applied across all I^3P contracts, NASA strives to attain maximum efficiencies while ensuring seamless, integrated services for IT customers.

Adoption of ITIL will enable NASA's mission by:

a. Better integrating the Agency's people, processes, and information.

b. Improving security.

c. Achieving efficiencies.

4.2 Implementation Plan and Scope for I^3P

NASA has developed an implementation plan and roadmap based on the introduction of ITIL v3 as the Agency's process framework in support of I^3P. Prospective service providers shall have documented, repeatable ITIL processes with relevant metrics reporting capabilities. NASA requires prospective service providers to engage and align with NASA's IT organization and NASA's ITIL processes.

NASA's approach is based on a phased implementation of ITIL processes. Activities in support of this implementation have been prioritized according to the following Government criteria:

a. Processes having greater relative importance to I^3P Acquisition Governance and Strategy.

b. Processes that require extensive, multiple vendor coordination and integration.

c. Processes that industry experience and best practice suggest should be addressed earlier in an ITIL implementation.

Twelve (12) of the ITIL v3 processes have been grouped into either Primary or Secondary implementation priorities.

Five (5) of these processes have been identified as primary implementation priorities. They include:

a. Change Management
b. Incident Management
c. Request Fulfillment
d. Problem Management
e. IT Service Level Management and IT Service Catalog Management*

*Service level management and Service Catalog Management processes were identified early as potential process development/refinement opportunities. Although preliminary documentation for those processes was developed, it was decided that an IT Configuration Management development/refinement effort should take priority and that Service Level Management and Service Catalog Management development/refinement efforts will be conducted along with second phase of process development/refinement events.

These five (5) processes are considered primary I^3P implementation priorities for the following reasons:

a. They are foundational processes in that many of the remaining ITIL processes depend on them.
b. They have strong ties to the ESD that was established in support of the I^3P acquisition and cross all the service contracts.
c. They tend to be ticket-management-heavy processes central to efficient and effective resolution of service interruptions and/or restoration of services to end-users.
d. There is stronger familiarity of these processes among the NASA technology groups.
e. There are significant opportunities associated with these processes for quick wins and/or accelerated achievement of I^3P objectives.

Seven (7) of the ITIL processes have been identified by NASA as secondary I^3P implementation priorities. They include:

a. Service Asset and Configuration Management
b. Release and Deployment Management
c. Capacity Management
d. Strategy Generation
e. Service Portfolio Management
f. Service Catalog Management
g. Supplier Management

In addition, Access Management has been identified as a process that, while implemented as part of ICAM Services, is targeted for closer integration with the Request Fulfillment process and tools implemented by the ESD.

These seven processes were targeted as secondary implementation priorities because:

a. Several (e.g. Release and Deployment Management and Capacity Management) require that Change Management be in place and operational prior to their implementation.
b. Several (Service Asset & Configuration Management and Service Catalog Management) require significant set-up and coordination across the I^3P contracts and delivery teams.
c. Several (Service Portfolio Management, Supplier Management and Strategy Generation) are critical to establishing strategic direction for I^3P and create momentum behind its execution.

The remaining fifteen (15) ITIL v3 processes are considered tertiary implementation priorities by NASA. Selection and prioritization of these for implementation will be evaluated and determined as the NASA ITIL framework matures. They include:

a. Demand Management
b. IT Financial Management
c. Information Security Management
d. Availability Management
e. Service Continuity Management
f. Validation and Testing
g. Transition Planning and Support
h. Knowledge Management
i. Event Management
j. Access Management
k. Operations Management
l. Service Evaluation
m. Service Improvement
n. Service Reporting
o. Service Measurement

In summary, NASA's introduction of ITIL v3 processes in support of the Agency's I^3P Acquisition supports the Agency's goals of transforming NASA's current environment to a more highly integrated IT Service Management environment.

4.3 NASA Defined ITIL v3 Process Requirements

I^3P contractors shall define and implement service delivery processes and procedures that are consistent with both individual service provider-specific and cross-functional performance work statement elements.

I^3P contractors shall implement processes and procedures that are consistent and complementary to NASA ITIL v3 aligned processes. All Contractor-developed processes and procedures necessary for the execution of the service delivery requirement are considered non-proprietary and shall be provided to the Government upon request.

I^3P Contractor interfaces associated with NASA IT services shall support NASA's ITIL process requirements as detailed in the cross-functional PWS elements, as well as any standards as identified in the Government process and policy documents associated with each NASA IT process.

Contractors shall actively participate in supporting changes to NASA process and policy documents. Changes to NASA process and policy documents will be managed by the Office of the Chief Information Officer.

The Government Incident Management system operated by the ESD for tracking the status of Problems, Incidents, changes, etc. will be the primary system of record used by the Government to track the status and completion of actions associated with these processes.

5 I^{3}P Common Architecture Components

5.1 Introduction and Overview

NASA's strategic approach to the management of IT infrastructure is to provide Enterprise-wide infrastructure services to maximize efficiency, improve IT security, and provide the best possible user experience. These infrastructure services have been defined into six (6) different portfolios:

a. End-User Services
b. Network and Communications Services
c. Enterprise Compute Services
d. Enterprise Applications
e. Web Services
f. Identity, Credential, and Access Management (ICAM) Services

Each of these portfolios provides a specific set of component services which comprise part of the NASA Enterprise Architecture as reflected in the NASA Enterprise Service Catalog. Common across these portfolio areas is the requirement for a TIER-0/1 ESD and an Enterprise Service Request System (ESRS). Finally, to reduce redundancy and promote interoperability and collaboration, applications within the NASA environment must be integrated through the NASA Application Portfolio Management process. Each of these elements of the NASA environment is further described below.

5.2 NASA Enterprise Architecture Repository

In support of the continual evolution of NASA EA, a knowledge base known as the NASA Enterprise Architecture Repository (NEAR) is being developed. The NEAR will support the alignment of IT goals, services, systems, components, and standards with Center, Mission Directorate, and Agency goals, while enabling more effective management of current assets and improved planning for new investments. In addition the NEAR will reduce information redundancy and improve data consistency while at the same time increasing flexibility and agility to provide a vision of the future state of the IT environment.

NASA's services are documented through a line-of-sight approach, i.e., from goals to functions to services to systems to components, with components as the lowest level of technical representation.

The NEAR will be hosted within the NASA IT environment. The NEAR will interface with repositories in IT Service areas and the Configuration Management Database (CMDB) at ESD as needed to provide authoritative data, especially at the system and component level.

Basic definitions of I3P services maintained in the Enterprise Service Request System (ESRS) will be provided to the NEAR from the NSSC via an electronic interface developed in accordance with the NEAR Interface Definition Specification (IDS).

5.3 NASA Enterprise Service Desk

The ESD is a foundational component of NASA's I^3P strategy for delivery of core IT infrastructure services. The ESD is located at and administered by NASA Shared Services Center (NSSC). The ESD serves as the single point of contact for Enterprise Services support providing a unified interface between the I^3P customers and the I^3P service providers (i.e. I^3P contracts – ACES, NICS, EAST, and WESTPRIME). The primary functions provided by the ESD include management of the IT Service Management (ITSM) software suite and ESD/ESRS CMDB, Tier 1 and Tier 0 incident management, service request processing, enterprise notification of planned/unplanned I^3P infrastructure outages, I^3P SLA metrics collection and reporting using the ITSM suite of tools, and integration support to the SIM and I^3P contractors for service continuity.

The ESD utilizes the ITIL v3 framework and associated processes common to all I^3P service providers as outlined in the cross-functional PWS elements defined in this document. ITIL processes are divided between Service Delivery and Service Support with the ESD serving as the primary point of contact between IT and users of IT services. The SIM organization in the OCIO ES&I Division is responsible for the definition and development of all NASA ITIL v3 processes. Service Support provides for implementation of operational processes and day-to-day management of the environment. Service Delivery is associated with the tactical processes and planning processes.

I^3P contractors shall interface with the ESD for a number of activities. These include (but are not limited to):

a. Building interfaces between the ESD Remedy system and the Contractor system. If the Contractor chooses to use the ESD's Remedy system, the Contractor is responsible for all integration work with the NSSC.

b. Resolving, statusing, and closing escalated incidents that cannot be resolved at the Tier 1 or Tier 0 level.

c. Providing and updating knowledge articles used by the ESD call agents to resolve and/or triage I3P Incidents that pertain to their specific contract service.

d. Providing notifications and community/organization lists for dissemination of planned and unplanned notices, service configuration changes affecting customers and/or other I3P Contractors.

    1. Providing status related to incident/problem resolution for those incidents assigned to their I^3P contract.
    2. Providing information as to any configuration changes related to I^3P service provisioning assigned to their I^3P contract.

3. Providing and updating knowledge articles for the Tier 0 self-service I^{3}P Web site for commonly identified incidents and or user self service activities (DRD 1294CF-014).
4. Providing a POC for ESD-to-I^{3}P-Contractor escalation processing of incidents/problem/service requests for both normal business and after hours.
5. Providing initial load of Configuration Items (CIs) to the ESD/ESRS CMDB during the transition period of the Contractor or in accordance with a specific contract Service Asset and Configuration Management Plan (DRD 1294CF-003).
6. Providing updates to the ESD/ESRS CMDB CIs e.g., for those items that were modified during the resolution of an incident or changed as a result of a scheduled refresh.

Important ESD reference information can be found in the following documents:

a. Enterprise Service Desk Concept of Operations
b. Enterprise Service Desk Performance Work Statement and associated Appendices
c. ESD/ESRS Interface Definition Specification
d. ESD/ESRS 7120.7 Program/Project Systems Requirements documents

These documents and other references are found at http://i3p.nasa.gov/document_file_home.cfm

5.4 NASA Enterprise Service Request System

To facilitate a seamless user experience, another element of the I^{3}P common architecture is the NASA ESRS. The ESRS includes:

a. A user-friendly, customer-facing interface to order all I^{3}P-provided services.
b. The ability to provide pricing for services offered.
c. Workflows to enable purchase authorization and verification of available funding.
d. Workflows to enable the efficient distribution of component orders to the appropriate I^{3}P service provider(s).
e. The ability for users to track the status of all orders via the Tier 0 web site.
f. A reporting capability to enable NASA leadership to monitor SLA performance and continuously improve service delivery.
g. Integration with the ESD to facilitate the aggregation of critical performance parameters with other I^{3}P metrics.

The ESRS utilizes the same IT Service Management software as the ESD ticket system (BMC/Remedy 7.5) and will support the ITIL service request processes detailed in the cross-

functional section of this PWS. Services and their attributes offered through the ESRS are defined and obtained from a web-based user interface that initiates workflow within Remedy.

I^{3}P contractors shall interface with the ESRS for a number of activities. These include:

a. Building interfaces between the ESRS Remedy system and the Contractor system during the transition period. If the Contractor chooses to use the ESD's Remedy system, the Contractor is responsible for all integration work with the NSSC.
b. Fulfilling, statusing, and closing service requests and updating CIs in the ESD/ESRS CMDB.
c. Providing a POC for ESRS-to-I^{3}P-Contractor interfacing/integration for both normal business and after-hours incident/problem resolution/service fulfillment.
d. Populating and updating I^{3}P services in the ESRS in accordance with the Remedy system requirements. The contractor shall carry this out via a web-based user interface that initiates workflow within Remedy. Contractor employees shall gain access to the system by requesting this specific role be provisioned using NAMS.

I^{3}P contractors receive I^{3}P service requests from the ESRS for fulfillment. The specific interface definition between the ESRS and I^{3}P contracts are defined in the ESD/ESRS Interface Definition Specification.

The ESRS is operational and can support the phase-in of all I^{3}P contracts. Contractors shall plan for a period of integration and testing to integrate any Contractor order fulfillment systems with the ESRS.

Important ESRS reference information can be found in the following documents:

a. Enterprise Service Desk Concept of Operations
b. Enterprise Service Desk Performance Work Statement and associated Appendices
c. ESD/ESRS Interface Definitions Specification
d. ESD/ESRS 7120.7 Program/Project Systems Requirements documents

These documents and other references are found at: http://i3p.nasa.gov/document_file_home.cfm

5.5 NASA Application Portfolio Management (APM)

Another critical element of the NASA environment is the management of NASA's Application Portfolios. NASA APM provides a framework that informs and facilitates decision making regarding application investment, development, maintenance, and decommissioning. This is accomplished by providing knowledge about available applications, application business and technical performance, and total cost of ownership.

In order to assist in effectively managing the NASA application landscape, Section 7 of this document includes process requirements associated with the NASA APM initiative.

In addition contractors shall comply with the following:

a. Provide an annual Application Inventory Cost report as documented in DRD 1294CF-005.

b. Review the NASA System for Tracking and Registering Applications and Websites (STRAW) to verify if an existing application will satisfactorily fulfill the stated application requirements prior to purchasing or developing a new application/capability and inform the Responsible NASA Official of said existing application(s).

c. Utilize the documented NASA ITIL process framework to ensure that all new applications being developed and/or entered into service are documented in STRAW and all applications being decommissioned/removed from service are so documented in STRAW.

6 Common Information Technology Security Requirements

6.1 Introduction and Overview

In order to appropriately secure NASA systems and information, the following IT security requirements apply to all I^{3}P Contractors. Where the term "information system" is used this refers to any system that physically or logically is connected to a NASA network, or that stores, processes, or transmits NASA data. Referenced NASA, federal, or IT Security policies or procedures may be downloaded from the NASA IT Security documentation website at http://itsecurity.nasa.gov/policies/index.html. Additional IT Security requirements may be contained in each service-specific I^{3}P contract and shall be in addition to the requirements contained in this cross-functional section.

6.2 Common IT Security Requirements

a. All information systems provided and/or operated under this contract are federal information systems. (A federal information system is defined in NIST SP 800-37, Rev 1 (and subsequent revisions), *Guide for the Security Authorization of Federal Information Systems* and in 40 U.S.C., Sec. 11331, as an information system used or operated by a federal agency, or by a Contractor of a federal agency or by another organization on behalf of a federal agency.) The contractor shall identify an IT Security POC for supporting IT security requirements for each I^{3}P contract. The contractor shall demonstrate compliance with IT information system security requirements by documenting a system security plan (DRD 1294CF-002.) The contractor shall be responsible for meeting the requirements for security authorization, also known as certification and accreditation (C&A), of these information systems, consistent with FIPS 200 and NIST SP 800-37 (Rev 1). A NASA official, determined in accordance with NPR 2810.1, will perform the role of the authorizing official for all such information systems.
   1. The contractor shall use NASA processes, as specified in NASA policy and procedures, to meet the requirements for security authorization of all such information systems.
   2. For all information systems provided under this contract that store, process or transmit NASA data, NASA will determine the system's FIPS 199 security categorization. For any other information systems provided under this contract or used in performing this contract, NASA will approve the system's FIPS 199 security category.
   3. The contractor shall ensure that all systems institute information security controls in accordance with NIST SP 800-53.
   4. The contractor shall support all applicable security assessments of each information system. At the discretion of the NASA authorizing official, the contractor shall either perform or provide for the performance of system security assessments, or support independent system security assessments (e.g., third party certification, IG Audits, GAO audits, and self certification), as part of the security authorization and continuous monitoring process.

5. The contractor shall track identified risks and security vulnerabilities for each information system in the NASA System Assessment and Authorization Repository (NSAAR) and remediate vulnerabilities on a schedule as determined by the NASA authorizing official.
6. All required system security documentation shall be entered into the NSAAR.

b. The contractor shall document their approach to managing information security in an Information Security Management Plan according to DRD 1294CF-001.

c. Some work performed by the I^3P contracts will require access to and/or generation of classified information, work in a secure area, or both, up to the level of Top Secret/ Secure Compartmented Information (TS/SCI). See Federal Acquisition Regulation clause 52.204-2 in this contract and DD Form 254 (refer to http://www.usaid.gov/policy/ads/500/dd254.pdf), Contract Security Classification Specification, Attachment [Insert the attachment number of the DD Form 254].
   1. The contractor shall ensure that key Contractor IT security personnel have the appropriate security clearances, up to the level of TS/SCI, to receive classified IT security threat information, to implement security controls based on such information, or to support other activities that require access to classified information.

d. The contractor shall configure and maintain operating system and software on all information systems provided under this contract in accordance with Federal and NASA security configuration policies and guidance.
   1. The contractor shall apply all relevant Federal system and software security configurations, for example, the Federal Desktop Core Configuration, according to NASA guidance.
   2. All information systems shall be patched with all critical patches (as determined by the product vendor or NASA) in accordance with the NASA Organization Defined Values for NIST SP 800-53 Security Controls and subsequent revisions.
   3. In some rare circumstances, the NASA Deputy CIO for IT Security or designee may determine that a particular patch must be applied more urgently. In such cases, all information systems shall be patched in the timeframe specified by the NASA Deputy CIO for IT Security or designee.
   4. System configurations and patching status for all information systems provided under and in support of this contract shall be reported using the NASA patch reporting environment. Each computer shall run up-to-date NASA reporting agent software for automated reporting. For any computers that cannot run the reporting agent software, a NASA-approved waiver must be obtained in accordance with NASA policy and procedures.

e. All information systems shall be protected by the NASA enterprise anti-malware (including anti-virus, anti-spyware, etc.) solution, which provides automated updates of virus definitions at least once every 24 hours and automated logging and reporting. The NASA enterprise anti-malware solution for desktops and laptops is provided by the ACES contract. For any computer that cannot use the anti-malware solution or for which no anti-malware software exists, a NASA-approved waiver must be obtained in accordance with NASA policy and procedures.
   1. The contractor shall correct or mitigate detected vulnerabilities in accordance with NASA policy, unless directed otherwise by NASA for specific urgent issues.

f. All information systems provided under this contract or used in support of this contract shall be scanned for vulnerabilities in accordance with NASA policy.
   1. The contractor shall make available all information systems located within the NASA network perimeter for network-based vulnerability scanning by NASA. NASA will coordinate scanning activities with the Contractor to the extent possible to ensure that vulnerability scanning creates minimal impact on operations.
   2. For all other information systems which process NASA data, the contractor shall report to NASA the results of vulnerability scans and remediation, in accordance with NASA guidance.

g. For all software developed in support of this contract, the contractor shall follow software security assurance practices to ensure that the software is designed and developed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects.
   1. The contractor shall verify that all software developers have been successfully trained in secure programming techniques.
   2. The contractor shall perform application security analysis and testing according to the verification requirements of an agreed-upon standard (such as the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS)).
   3. For web applications, the contractor shall ensure that the software shall not include any of the flaws described in the current "OWASP Top Ten Most Critical Web Application Vulnerabilities."

h. The contractor shall follow NASA IT security incident management procedures in accordance with NASA policies and ensure coordination of its incident response team with the NASA Security Operations Center (SOC). The contractor shall report (DRD 1294CF-012) to the NASA SOC any suspected computer or network security incidents occurring on any systems, in accordance with Federal mandates and NASA policies and procedures. The contractor shall provide all necessary assistance and access to the affected systems so that a detailed investigation can be conducted, problems remedied, and lessons learned documented. Security logs and audit information shall be handled according to evidence preservation procedures.
   1. The contractor shall make available logs from any information system to the NASA common logging environment, as requested by the NASA SOC. Electronic raw log data shall be forwarded from the source device to the NASA common logging environment, in accordance with NASA policies, procedures and guidance.
   2. The contractor shall report the theft or loss of any device that may contain NASA information, in accordance with NASA incident reporting policy and procedures.

i. The contractor shall provide a logging environment that centrally captures and retains logs from all information systems provided under this contract.

j. The contractor shall provide to NASA real-time, electronic access to all asset information and configuration management information for all devices provided under this contract and in support of this contract.

k. The contractor shall ensure that all individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by a system administrator, possess knowledge appropriate to those tasks, as demonstrated by holding industry-standard certifications. In addition, system administrators shall not be granted elevated privileges to information systems covered under this contract unless they are authorized and have met the training requirements in accordance with NASA policy.

l. Prior to deployment of any IT security services, the contractor shall obtain approval from the NASA Deputy CIO for IT Security or designee. Any IT security services provided by the contractor shall be coordinated and integrated with the NASA SOC.
    1. Monitoring NASA networks (NASA IP Address space) is an IT security service performed by the NASA SOC (both security monitoring of network traffic and monitoring of system logs) and will be done only by the SOC unless otherwise agreed upon by the I^3P Contractor and NASA and documented in the Contractor's Information Security Management Plan.

m. The contractor shall support the integration of NASA SOC IT security services and technologies into systems provided under this contract and in support of this contract, in accordance with NASA guidance.

n. The contractor shall work with the NASA OCIO and the incumbent contractor to transfer responsibility for all IT security requirements for existing information systems within the scope of the contract from the incumbent contractor to the successor contractor. The contractor will receive from NASA a list of the applicable information systems.

7 Cross Functional Performance Work Statement Elements

The NASA IT Infrastructure Integration Program (I^3P) requires coordination, collaboration, and ultimately co-management of key processes across I^3P Service contractors and contract boundaries. To ensure a successful integrated IT service environment across NASA, it is essential that IT service providers adhere to the NASA ITIL framework. The purpose of the following CF-PWS Elements are to consolidate the requirements that must remain consistent across contractor service agreements. The requirements contained in this section are the responsibilities of the contractor or contractors associated with the Cross Functional Services.

7.1 General Provisions

7.1.1 IT Infrastructure Library® Version 3 (ITIL® v3) Support

The contractor shall be responsible for:

a. Defining and implementing service delivery processes and procedures that are consistent with the requirements contained in this CF-PWS. Contractor processes used to provide services shall be consistent and complimentary with Government ITIL® v3 aligned processes.
b. Ensuring that interfaces with Government, I^3P contractors and other contractors are consistent with Government ITIL® v3 aligned processes.
c. Ensuring that changes are approved and authorized by Government in accordance with Government Change Management Process.
d. Providing information to support maintenance of Government Enterprise Service Catalog.

7.1.2 Understanding and Knowledge of ITIL®

The contractor shall be responsible for:

a. Ensuring that all contractor personnel involved in delivery of services shall possess basic knowledge, understanding, and familiarity with foundational ITIL v3 concepts and processes.
b. Providing verification that contractor personnel, required in delivery of services, are experienced and trained in ITIL.
c. Participating in an objective assessment of contractor ITIL maturity.

7.2 Change Management

7.2.1 High-Level Process Flow Diagram, Goal, Purpose and General

Goal: The goals of Change Management are to: Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and re-work; and respond to business and IT requests for change that will align services to business needs.

Purpose: The purpose of Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of changes, changes to service assets and CIs are recorded in the Configuration Management Data Base (CMDB), and overall business risk is optimized.

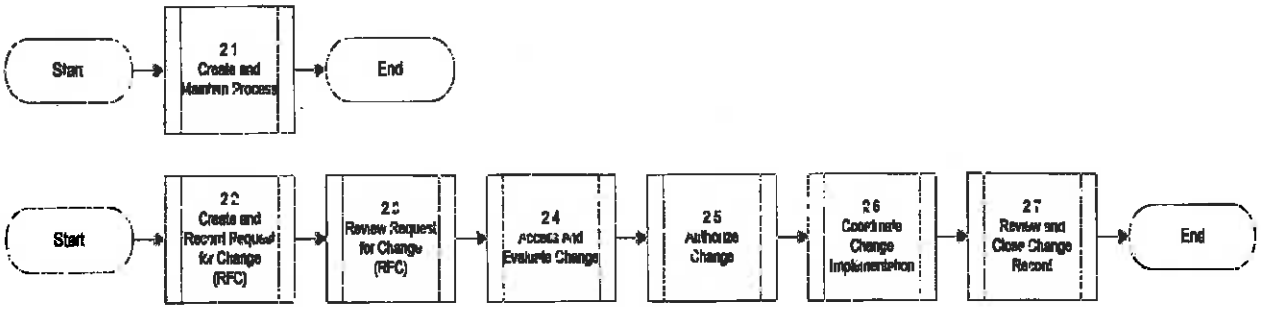

Figure 8: High-Level Change Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing Change Management procedures that align with Government Change Management Process.
b. Documenting, tracking and managing all Changes using a contractor or Government provided Change Management system.
c. (When contractors use a contractor Change Management System) Providing integration between contractor and Government Change Management systems including the integration of applicable software, e-mail and telephony in accordance with Government Change Management Process. All changes necessary to provide system integration shall be made at the contractor's expense. The contractor's solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
d. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through resolution in accordance with Government Change Management Process.
e. Providing case ownership of Change Requests that are assigned to the contractor until Change record is closed or ownership is officially recorded and subsequently reassigned.
f. Participating in regularly scheduled Change Management meetings in accordance with Government Change Management Process.

7.2.2 Create and Maintain Change Management Process

The contractor shall be responsible for:

a. Complying with Government Change Management Process.

b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Change Management process.

7.2.3 Create and Record Request for Change (RFC)

The contractor shall be responsible for:

a. Determining type of change request that is required in accordance with Government Change Management Process
b. Determining change procedures to be used in accordance with Government Change Management Process.
c. Completing request for change form(s) (e.g. performing data entry into the government's change management system thereby creating a Change Request), with required documentation in accordance with Government Change Management Process.

7.2.4 Review Request for Change (RFC)

The contractor shall be responsible for providing information for preliminary review of requests for change.

7.2.5 Assess and Evaluate Change

The contractor shall be responsible for:

a. Providing information to support impact assessment of requests for change.
b. Providing information to support categorization and risk assessment of requests for change
c. Providing information to support assessment of the benefit of implementing requests for change.

7.2.6 Authorize Change

The contractor shall be responsible for:

a. Obtaining Government authorization for changes to services or underlying infrastructure supporting services in accordance with Government Change Management Process.
b. Participating in Change Advisory Board(s) in accordance with Government Change Management Process.

7.2.7 Coordinate Change Implementation

The contractor shall be responsible for:

a. Developing change implementation procedures in accordance with Government Change Management Policy.

b. Coordinating activities with Government, I^3P contractors and other contractors to implement approved changes.

7.2.8 Review and Close Change Record

a. The contractor shall be responsible for providing information and participating in review meetings for closure of change records and capture of lessons learned.
b. The contractor shall have responsibility for documenting in the government Change Request (CR) tracking system relevant CR closure information for which the contractor had the lead in implementation.
c. The contractor shall be responsible for subsequent CR closure updates.

7.3 Incident Management

7.3.1 High-Level Process Flow Diagram, Goal and General Provisions

Goal: The primary goal of Incident Management is to restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. "Normal service operation" is defined here as service operation within Service Level Agreement (SLA) limits.

Purpose: The purpose of Incident Management is to deal with all unplanned interruptions to an IT service or a reduction in the quality of IT service. This can include failures; questions or queries reported by users via telephone, email, face to face, or automatically detected and reported by event monitoring tools.

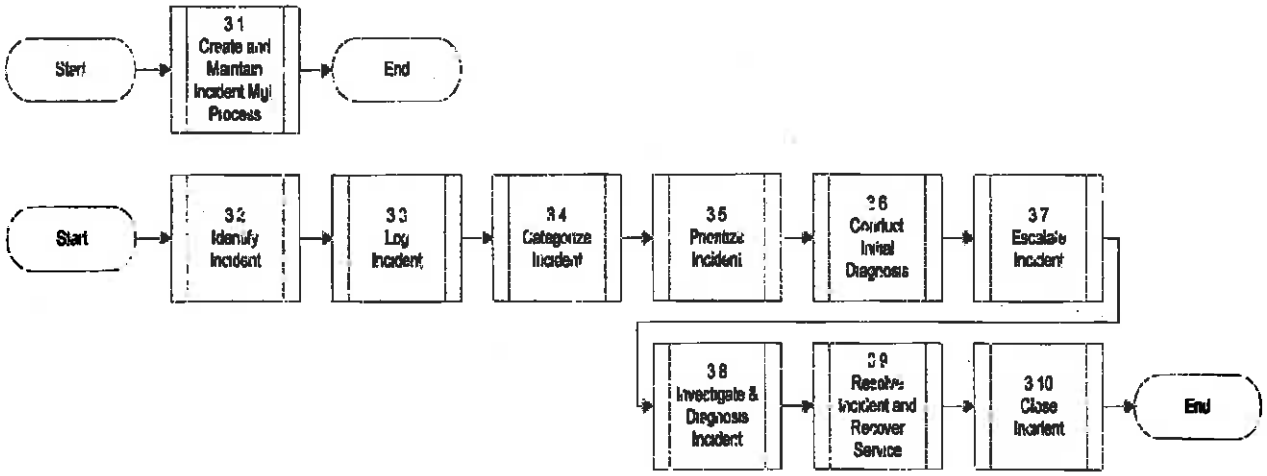

Figure 9: High-Level Incident Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing Incident Management procedures that align with Government Incident Management Process.
b. Documenting, tracking and managing all Incidents using a contractor or Government provided Incident Management system.
c. (When contractors use a contractor Incident Management System) Providing integration between contractor and Government Incident Management systems including the integration of applicable software, e-mail and telephony in accordance with Government Incident Management Process. All changes necessary to provide system integration shall be made at contractor expense. Contractor solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
d. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through Incident resolution in accordance with Government Incident Management Process.
e. Providing case ownership of Incidents that are assigned to contractor until service is restored or ownership is reassigned.
f. Retaining ownership of each Incident assigned to contractor by the Enterprise Service Desk.
g. Assigning end-to-end responsibility of each Incident to a single point of contact in order to facilitate communications with Government until service is restored.
h. Resolving assigned Incidents in collaboration and coordination with Government, I^3P contractors and other Contractors, and in accordance with Government Incident Management Process.
i. Complying with Government notification and escalation procedures in accordance with Government Incident Management Process.
j. Participating in daily Incident review meetings.

k. Implementing and supporting continuous improvement actions to reduce frequency and severity of reported Incidents.

7.3.2 Create and Maintain Incident Management Process

The contractor shall be responsible for:

a. Complying with Government Incident Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Incident Management process.

7.3.3 Identify Incident

The contractor shall be responsible for:

a. Detecting Incidents via both manual and automated monitoring mechanisms.
b. Notifying Enterprise Service Desk of an Incident within 15 minutes of detection.

7.3.4 Log Incident

The contractor shall be responsible for:

a. Logging Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure Incidents are logged in accordance with Government Incident Management Process.

7.3.5 Categorize Incident

The contractor shall be responsible for:

a. Categorizing Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure Incidents are categorized in accordance with Government Incident Management Process.

7.3.6 Prioritize Incident

The contractor shall be responsible for:

a. Prioritizing Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure Incidents are prioritized in accordance with Government Incident Management Process.

7.3.7 Conduct Initial Diagnosis

The contractor shall be responsible for:

a. Conducting initial diagnosis of Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure initial diagnosis of Incidents is performed in accordance with Government Incident Management Process.

7.3.8 Escalate Incident

The contractor shall be responsible for:

a. Providing Tier 2 and Tier 3 Incident resolution and support.
b. Accepting Incident Lead role as assigned.
c. Providing a mechanism for expedited handling of Incidents that are of high business priority to Government in accordance with Government Incident Management Process.
d. Opening 'Child' Incident records for other I^3P Contractor(s).
e. Providing status updates to Government Incident Management System.

7.3.9 Investigate and Diagnose Incident

The contractor shall be responsible for:

a. Conducting incident investigation and diagnostic activities to identify root cause and develop Incident work-around(s).
b. Executing Incident Management in accordance with Government Incident Management Procedures.

7.3.10 Resolve Incident and Recover Service

The contractor shall be responsible for:

a. Applying resolution or work around to restore service as quickly as possible.
b. Accomplishing resolution and recovery of all Incidents reassigned to Tier 2 and/or Tier 3 for support.
c. Notifying Enterprise Service Desk via Incident Management System that service is restored.
d. Recommending implementation of measures to avoid reoccurrence of Incidents relating to Services in accordance with Incident Management Procedures.

7.3.11 Close Incident

a. The contractor shall be responsible for providing Incident closure information in accordance with Government Incident Management Process.
b. The contractor shall have responsibility for documenting in the government Incident Management tracking system relevant incident closure information for which the contractor had the lead in implementation.
c.

Request Fulfillment

7.4.1 High-Level Process Flow Diagram and General Provisions

Goal: The goals of Request Fulfillment are: provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists; provide information to users and customers about the availability of services and the procedure for obtaining them; source and deliver components of requested standard services; and assist with general information, complaints or comments.

Purpose: The purpose of Request Fulfillment is to deal with Service Requests from users whether small (i.e., low risk, frequently occurring, low cost (e.g. a request to change a password, a request to install additional software onto a particular workstation, and a request to relocate some items of a desktop)) or large – higher risk, less frequently occurring, higher cost (e.g. a request to replace major infrastructure or other service components or a request to refresh major software components)).

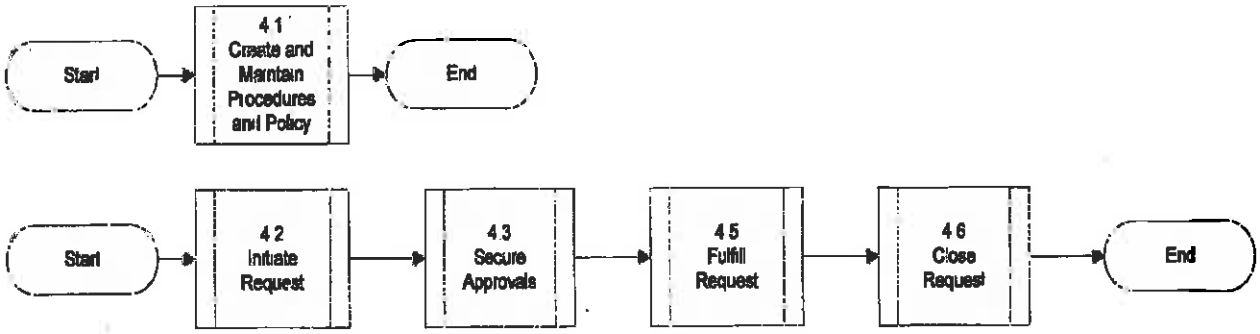

Figure 10: High-Level Request Fulfillment Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing Request Fulfillment procedures that align with Government Request Fulfillment Process.
b. Documenting, tracking and managing all Requests using a contractor or Government provided Request Fulfillment system.
c. (When contractors use a contractor Request Fulfillment System) Providing integration between contractor and Government Request Fulfillment systems including integration of applicable software, e-mail and telephony in accordance with Government Request Fulfillment Process. All changes necessary to provide system integration shall be made at the contractor's expense. The contractor's solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).

d. Maintaining communications regarding Request status with users at each status change via Enterprise Service Desk from time a Request is identified, through closure and through any follow-up communication.
e. Providing case ownership of Requests that are assigned to Contractor until Request is closed.
f. Participating in Request Fulfillment review meetings.
g. Implementing and supporting continuous improvement of Request Fulfillment through self-service or other mechanisms.

7.4.2 Create and Maintain Request Fulfillment Process

The contractor shall be responsible for:

a. Complying with Government Request Fulfillment Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Request Fulfillment process.

7.4.3 Initiate Request

The contractor shall be responsible for:

Utilizing Government-provided Enterprise Service Request System to define services that customers may request.

7.4.4 Secure Approvals

The contractor shall be responsible for providing supporting information on all Requests in support of approvals in conformance with Government Request Fulfillment Process. Supporting information includes, but is not limited to, price quotes, delivery SLAs, and dependencies.

7.4.5 Fulfill Request

The contractor shall be responsible for:

a. Fulfilling all Requests within Government Service Level Agreements as defined for each standard Request and in conformance with Government Request Fulfillment Process.

b. Enabling fulfillment of a Request in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with Government Request Fulfillment Process.
c. Providing accurate and regular status updates for all Requests assigned to the contractor via the Enterprise Service Desk in accordance with Government Request Fulfillment Process.

7.4.6 Close Request

a. The contractor shall be responsible for providing Request closure information in accordance with Government Request Fulfillment Process.

b.

7.5 Problem Management

7.5.1 High-Level Process Flow Diagram and General Provisions

Goal: The primary goals of Problem Management are: to prevent problems and resulting Incidents from happening, to eliminate recurring Incidents and to minimize the impact of Incidents that cannot be prevented.

Purpose: The purpose of Problem Management is to provide a pre-defined and approved process for managing the lifecycle of all Problems to include diagnosis, determination of resolutions to those Problems, implementing solutions through appropriate control and change management procedures and preventing Problem reoccurrence.

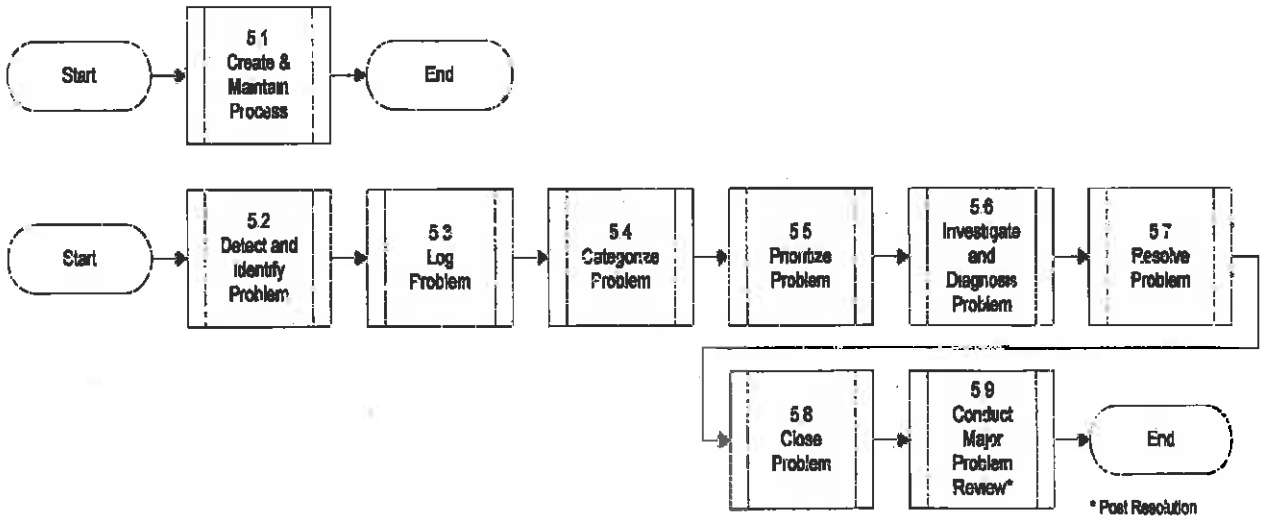

Figure 11: High-Level Problem Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing Problem Management procedures that align with Government Problem Management Process.

b. Documenting, tracking and managing all Problems in a Government Problem Management System.
c. (When contractors use a contractor Problem Management System) Providing integration between the contractor and Government Problem Management systems including integration of applicable software, e-mail and telephony in accordance with Government Problem Management Process. All changes necessary to provide system integration shall be made at the contractor's expense. Contractor solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
d. Retaining ownership of each problem assigned to the contractor by either ESD or SIM.
    1. To the extent a Problem does not arise from or relate to the Contractor's Services:
    a) The contractor shall notify ESD in accordance with Government Problem Management Procedures.
    b) The contractor shall maintain responsibility for the Problem until the Problem is reassigned by ESD or SIM.
e. Assigning end-to-end responsibility of each Problem to a single point of contact in order to facilitate communications with Government.
f. Monitoring, controlling and managing each Problem assigned to contractor until it is closed by Enterprise Service Desk.
g. Resolving assigned Problems in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with Government Problem Management Process.
h. Complying with Government notification and escalation procedures in accordance with Government Problem Management Process.

7.5.2 Create and Maintain Problem Management Process

The contractor shall be responsible for:

a. Complying with Government Problem Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Problem Management process.

7.5.3 Detect and Identify Problem

The contractor shall be responsible for:

a. Identifying Problems by proactively performing on-going trend analysis on Incident information.
b. Detecting Problems via both manual and automated monitoring mechanisms.

7.5.4 Log Problem

The contractor shall be responsible for:

a. Logging Problems in accordance with Government Problem Management Process.

b. Providing information to ESD to ensure Problems are logged in accordance with Government Problem Management Process.

7.5.5 Categorize Problem

The contractor shall be responsible for:

a. Categorizing Problems in accordance with Government Problem Management Process.
b. Providing information to Enterprise Service Desk to ensure Problems are categorized in accordance with Government Problem Management Process.

7.5.6 Prioritize Problem

The contractor shall be responsible for:

a. Prioritizing Problems in accordance with Government Problem Management Process.
b. Providing information to Enterprise Service Desk to ensure Problems are prioritized in accordance with Government Problem Management Process.

7.5.7 Investigate and Diagnose Problem

The contractor shall be responsible for:

a. Conducting Problem investigation in accordance with Government Problem Management Process.
b. Conducting Problem diagnostics in accordance with Government Problem Management Procedures.
c. Providing status tracking information in Government Problem Management System in accordance with Government Problem Management Process.
d. Investigating and diagnosing Problems in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with Government Problem Management Process.
e. Validating Problem workarounds.
f. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through Problem resolution in accordance with Government Problem Management Process.
g. Performing Root Cause Analysis (RCA) in accordance with Government Problem Management Procedures.
h. Updating Known Error information in accordance with Government Problem Management Process.
i. Documenting problem resolution in accordance with Government Problem Management Process.
j. Developing a Corrective Action Plan in accordance with Government Problem Management Process.

7.5.8 Resolve Problem

The contractor shall be responsible for:

a. Determining if initiation of Change Management Process is required.
b. Generating requests for change for permanent solutions and corrective action plans in accordance with Government Change Management Process.
c. Applying resolutions across the enterprise, as applicable.
d. Implementing the approved corrective action plan with follow-up to eliminate the fault from the operating environment.
e. Resolving Problems in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with Government Problem Management Process.
f. Developing supporting documentation, scripts, and procedures for Enterprise Service Desk to facilitate resolution of repetitive problems (DRD 1294CF-014). These supporting elements shall be fully developed, documented and tested prior to release in accordance with ITIL v3 Change, Release, and Deployment processes.

7.5.9 Close Problem

a. The contractor shall be responsible for Providing Problem resolution and closure information in Government Problem Management System in accordance with Government Problem Management Process.
b. The contractor is responsible for Problem Management system ticket closure and subsequent updates to the government Problem Management system regarding previously assigned and closed Problem Management tickets.

7.5.10 Conduct Major Problem Review

The contractor shall be responsible for:

a. Participating in major Problem reviews.
b. Providing Problem resolution details.

7.6 Service Level Management (SLM)

7.6.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Service Level Management is to ensure that an agreed-upon level of service is provided for all IT services, and that future services are delivered in accordance with Service Level Agreements. Proactive measures are also taken to seek and implement improvements to the level of service delivered.

Purpose: The purpose of SLM is to ensure that all operational services and their performance are managed in a consistent manner throughout the IT organization to meet the needs of the business and customers.

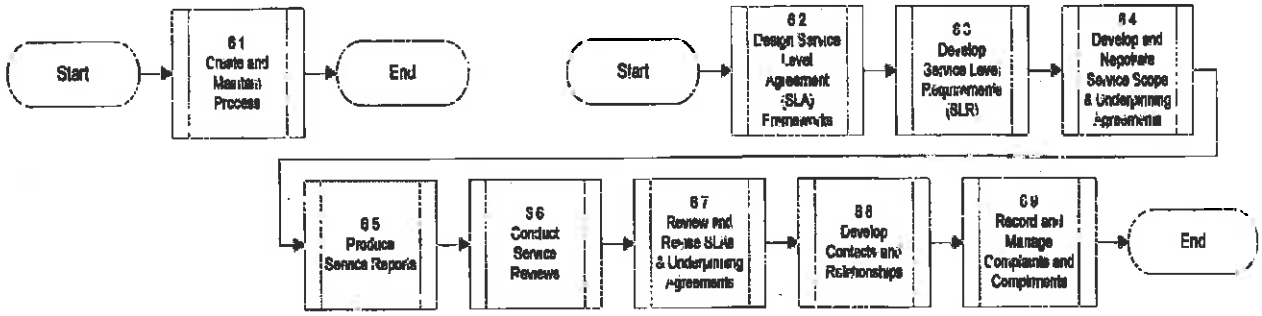

Figure 12: High-Level Service Level Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for designing and implementing SLM procedures that align with Government SLM Process.

7.6.2 Create and Maintain SLM Process

The contractor shall be responsible for:

a. Complying with the approved Government SLM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government SLM process.

7.6.3 Design Service Level Agreement (SLA) Frameworks

The contractor shall be responsible for providing information to support design and development of Service Level Agreement frameworks.

7.6.4 Develop Service Level Requirements (SLR)

The contractor shall be responsible for providing information to support Government with developing Service Level Requirements and gaining agreement with Government IT services customers.

7.6.5 Develop and Negotiate Service Level Scope and UnderpinningAgreements

The contractor shall be responsible for providing information to support Government with developing and drafting service level scope and underpinning agreements.

7.6.6 Produce Service Level Reports

The contractor shall be responsible for providing information to support Government reporting of Service Levels in accordance with Government SLM Process.

7.6.7 Conduct Service Reviews

The contractor shall be responsible for supporting Government service reviews (e.g., meetings) in accordance with Government SLM Process.

7.6.8 Review and Revise Service Level Agreements and Underpinning Agreements

The contractor shall be responsible for providing information to support Government with reviewing and revising Service Levels and underpinning agreements.

7.6.9 Develop Contacts and Relationships

The contractor shall be responsible for providing information to support Government with developing customer relationships as it relates to IT services, service performance, and service agreements.

7.6.10 Record and Manage Customer Service Level Feedback

The contractor shall be responsible for:

a. Providing information to support Government with assigning and dispositioning actions related to customer feedback.

7.7 Service Asset and Configuration Management (SACM)

7.7.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goals of SACM are to support the business and customer's control objectives and requirements, support efficient and effective Service Management processes by providing accurate configuration information to enable people to make decisions at the right time (e.g., to authorize change and releases and to resolve incidents and problems faster), minimize the number of quality and compliance issues caused by improper configuration of services and assets, and optimize service assets, IT configurations, capabilities and resources.

Purpose: The purpose of SACM is to identify, control, record, report, audit and verify Service Assets and CIs, including versions, baselines, constituent components, and their attributes and relationships, account for, manage, and protect the integrity of Service Assets and CIs (and where appropriate, those of their customers) throughout the service lifecycle.

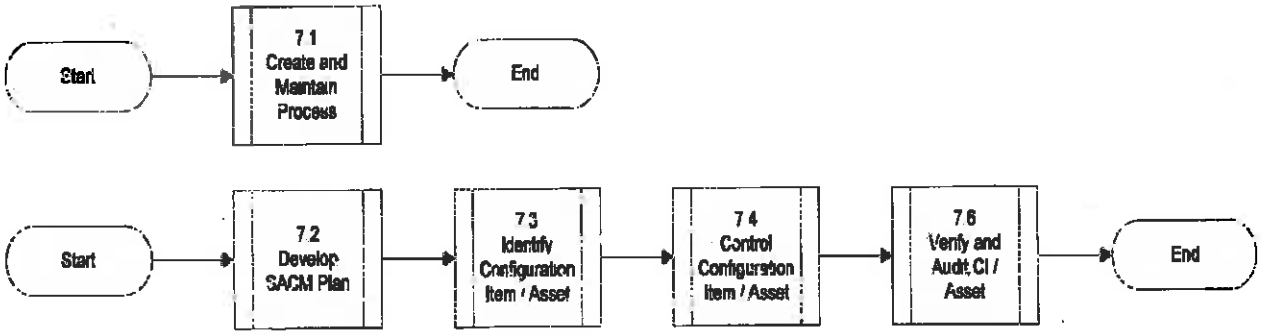

Figure 13: High-Level Service Asset and Configuration Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Defining and implementing contractor SACM procedures in accordance with Government SACM Process.
b. Documenting, tracking and managing all Service Assets and CIs in Government CMDB in accordance with Government SACM Process.

c. (When contractors use a contractor CMDB System) Providing integration between the contractor and Government CMDB systems including integration of applicable software, e-mail and telephony in accordance with Government SACM Process. All changes necessary to provide system integration shall be made at the contractor's expense. The contractor solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
d. The Government CMDB is the official and authoritative system of record for all CIs (CI) where it is determined to be in the best interests of the government to track such. The contractor is responsible for creating, maintaining, and updating (to include proper removal) of CMDB records in the Government CMDB for CIs under their purview. Archival records shall be maintained for all CIs deleted from the CMDB.

7.7.2 Create and Maintain Service Asset and Configuration Management (SACM) Process

The contractor shall be responsible for:

a. Complying with Government SACM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government SACM process.

7.7.3 Develop Service Asset and Configuration Management (SACM) Plan

The contractor shall be responsible for developing and maintaining SACM Plan in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with DRD 1294CF-003.

7.7.4 Identify CI / Asset

The contractor shall be responsible for:

a. Developing a strategy for ensuring identification of all CIs in accordance with Government SACM Process.
b. Identifying and labeling, as applicable, all CIs in accordance with Government SACM Process
c. Assigning unique identifiers to each CI in accordance with Government SACM Process.
d. Specifying relevant attributes, relationships, owner and baselines for each CI in accordance with Government SACM Process.

7.7.5 Control CI / Asset

The contractor shall be responsible for:

a. Identifying when a change to a CI is necessary and initiating a request for change in accordance with Government Change Management Process.

b. Determining and reporting the root cause, impact, and actions to prevent recurrence of an unauthorized change in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with Government SACM Process.

7.7.6 Verify and Audit CI / Asset

The contractor shall be responsible for:

a. Participating in Government audit activities to ensure conformity between documented CIs and actual CIs in accordance with Government SACM Process.
b. Providing audit CI data and Release documentation in accordance with Government SACM Process.
c. Implementing corrective actions in accordance with Government SACM Process.
d. Providing information to support audit reporting in accordance with Government SACM Process.

7.8 Release and Deployment Management (RDM)

7.8.1 High Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Release and Deployment Management is to deploy releases into production and establish effective use of the service.

Purpose: The purpose of Release and Deployment Management is to: define and agree on release and deployment plans with customers and stakeholders; ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the Configuration Management Database (CMDB); ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate; and ensure that customers and stakeholder change is managed during Release and Deployment activities.

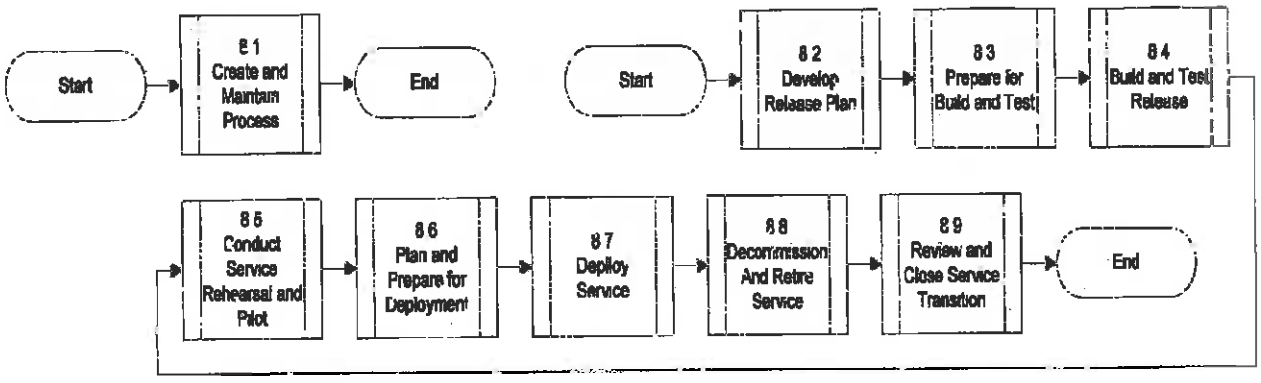

Figure 14: High-Level Release and Deployment Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for performing Releases in accordance with Government Release and Deployment Process.

7.8.2 Create and Maintain Release and Deployment Management Process

The contractor shall be responsible for:

a. Complying with Government RDM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government RDM Process.
c. Conducting an annual inventory of applications being used to support NASA services, and report this data, including the cost to develop, operate, enhance and maintain applications as specified in DRD 1294CF-005.
d. Reviewing the NASA Application Repository to verify if an existing application will satisfactorily fulfill the stated application requirements prior to purchasing or developing a new application/capability and inform the Responsible NASA Official of said existing application(s).

7.8.3 Develop Release Plan

The contractor shall be responsible for developing and maintaining RDM Plan in collaboration and coordination with Government, I^3P Contractors, and other contractors and in accordance with DRD 1294CF-004.

7.8.4 Prepare for Release Build and Test

The contractor shall be responsible for preparing for release build and test in collaboration and coordination with Government, I^3P contractors and other Contractors.

7.8.5 Build and Test Release

The contractor shall be responsible for:

a. Building and testing releases in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with Government RDM Process.
b. Developing release documentation in accordance with Government RDM Process.
c. Creating test scenario and acceptance criteria and submitting them for review in accordance with Government RDM Process.
d. Managing Release build and test environments.

7.8.6 Conduct Service Rehearsal and Pilot

The contractor shall be responsible for conducting service rehearsals and pilots in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.

7.8.7 Plan and Prepare for Deployment

The contractor shall be responsible for:

a. Planning and preparing for deployment in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.
b. Assessing the need for and planning for a release stabilization period in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.

7.8.8 Deploy Service

The contractor shall be responsible for:

a. Deploying services in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.
b. Verifying successful service deployment in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.
c. Executing back-out plan, if necessary, in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.

7.8.9 Decommission and Retire Service

The contractor shall be responsible for decommissioning and retiring services in collaboration and coordination with Government, I^{3}P contractors and other contractors and in accordance with Government RDM Process.

7.8.10 Review and Close Service Release Deployment

The contractor shall be responsible for closing release deployment in accordance with Government RDM Process.

7.9 Capacity Management

7.9.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Capacity Management process is to ensure IT capacity in all areas of IT is matched to the needs of the Government's business.

Purpose: The purpose of Capacity Management is to provide a point of focus and management for all capacity and performance related issues, relating to both services and resources.

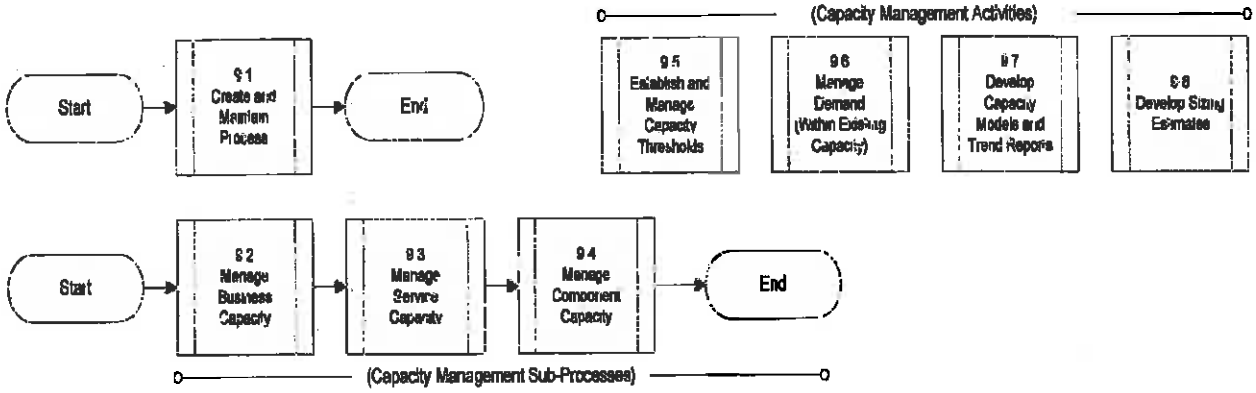

Figure 15: High-Level Capacity Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing Capacity Management procedures that align with Government Capacity Management Process.
b. Developing and maintaining Capacity Management Plan in collaboration and coordination with Government, I^3P Contractors, and other contractors and in accordance with DRD 1294CF-006.
c. Conducting annual reviews of projected capacity requirements for infrastructure and related services, and providing recommendations based upon information provided by Government Portfolio Management Process as part of Government's normal business planning cycle.

7.9.2 Create and Maintain Capacity Management Process

The contractor shall be responsible for:

a. Complying with Government Capacity Management Process.

b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Capacity Management Process.

7.9.3 Manage Business Capacity

The contractor shall be responsible for:

a. Providing impact assessment of potential business capacity issues based on Government business direction.
b. Prototyping and sizing capacity impact solutions, including:
    1. Developing and maintaining standard templates for capacity test plans in collaboration and coordination with Government, I^3P contractors and other Contractors.
    2. Coordinating tests with Government, I^3P contractors and other contractors to provide end-to-end testing.
    3. Testing and sizing models for capacity impacts.
c. Developing plans for required changes to existing capacity in accordance with DRD 1294CF-006.

7.9.4 Manage Service Capacity

The contractor shall be responsible for:

a. Providing SOM with information regarding Service Capacity and issues.
b. Monitoring Service Capacity including:
    1. Collecting Service Capacity performance data, at a minimum, per the following schedule:
        a) Daily data collection for volatile and dynamic systems.
        b) Weekly data collection for variable and stable systems.
    2. Maintaining Services aligned with Government Enterprise Service Catalog.
c. Analyzing Service Capacity, including:
    3. Providing service capacity performance reports in accordance with DRD 1294CF-007.
d. Tuning Service performance, including changing capacity, to take corrective action or adjust for more effective usage.
e. Establishing capacity thresholds and making adjustments based on Government requirements.
f. Responding to Government requests for capacity impact statements within 30 days.

7.9.5 Manage Component Capacity

The contractor shall be responsible for:

a. Providing SOM with information regarding component capacity and issues.
b. Monitoring component capacity usage, including:
    1. Maintaining components aligned with Government CMDB.

c. Analyzing component usage, including:
   1. Reviewing component capacity data.
   2. Determining if proactive changes are needed.
   3. Determining if tuning or replacing a component can provide for a more effective use of the component.
d. Tuning or replacing components, including:
   1. Adjusting or balancing component capacity to provide more effective usage.
   2. Changing component capacity to correct utilization issues.
   3. Replacing components in compliance with Change Management Process.
   4. Collecting and providing component capacity data based on Government-specified standards and metrics.
e. Providing component capacity reports in accordance with DRD 1294CF-007.
f. Reviewing, validating and updating component baselines and profiles in the CMDB.

7.9.6 Establish and Manage Capacity Thresholds

The contractor shall be responsible for monitoring and generating alerts and warnings associated with capacity and performance thresholds.

7.9.7 Manage Demand (within existing capacity)

The contractor shall be responsible for providing information and support to manage demand within existing capacity levels.

7.9.8 Develop Capacity Models and Trend Reports

The contractor shall be responsible for providing capacity models and trend reports in accordance with DRD 1294CF-007.

7.9.9 Develop Sizing Estimates

The contractor shall be responsible for developing sizing estimates to support capacity planning.

7.10 Availability Management

7.10.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The Goal of Availability Management is to ensure that the level of service availability delivered in all services is matched to the requirements of the Government's business.

Purpose: The Purpose of Availability Management is to provide a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved.

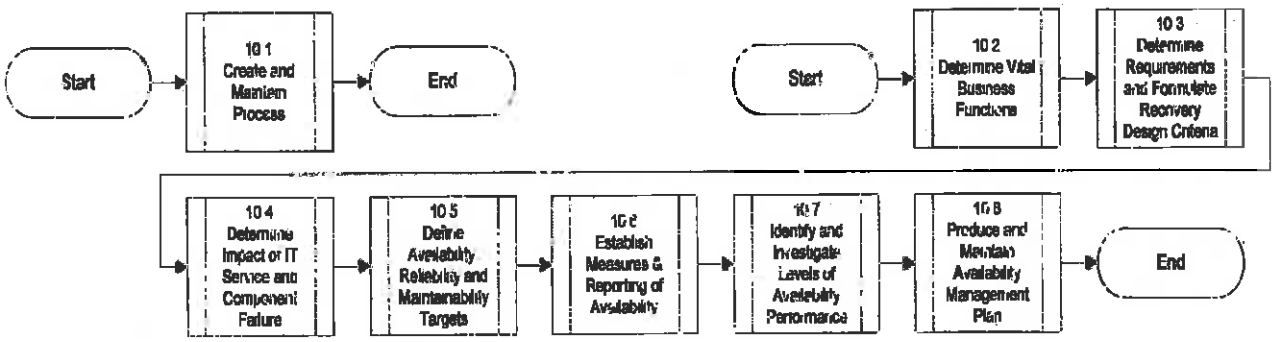

Figure 16: High-Level Availability Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for designing and implementing Availability Management procedures that align with Government Availability Management Process.

Identifying planned downtime and scheduling downtime in collaboration and coordination with Government, I^3P contractors and other contractors and in alignment with Government Mission Flight Requirements.

7.10.2 Create and Maintain Availability Management Process

The contractor shall be responsible for:

a. Complying with Government Availability Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Availability Management Process.

7.10.3 Determine Vital Business Functions

The contractor shall be responsible for providing information to support Government with identifying vital business functions.

7.10.4 Determine Requirements and Formulate Recovery Design Criteria

a. The contractor shall be responsible for providing information to support Government with defining availability requirements.
b. Providing information to support Government with formulating recovery design criteria.

7.10.5 Determine Impact of IT Service and Component Failure

The contractor shall be responsible for providing information to support Government with conducting business and service impact analysis and component failure impact analysis related to availability.

7.10.6 Define Availability, Reliability and Maintainability Targets

The contractor shall be responsible for providing information to support Government with developing and maintaining availability, reliability and maintainability targets and measures that align with applicable Service Level Agreements.

7.10.7 Monitor and Analyze Availability, Reliability and Maintainability

The contractor shall be responsible for:

a. Establishing service metrics and tools for measuring availability, reliability and maintainability in accordance with Government Availability Management Process.
b. Deploying tool sets and/or interfaces to permit end-to-end measurement of availability.
c. Collecting and recording availability, reliability and maintainability data.
d. Monitoring availability, reliability and maintainability elements with respect to Service Levels.
e. Conducting analysis for compliance with availability, reliability and maintainability Service Levels.
f. Reporting results of monitoring and analysis in accordance with DRD 1294CF-009.
g. Providing information to assist in Problem analysis related to service availability.

7.10.8 Identify and Investigate Levels of Availability Performance

The contractor shall be responsible for:

a. Identifying Availability performance that fails to meet Government Service Level Agreements.
b. Investigating availability performance that fails to meet Government Service Level Agreements.
c. Initiating actions to ensure availability performance complies with Government Service Level Agreements.

7.10.9 Produce and Maintain Availability Management Plan

The contractor shall be responsible for:

a. Developing and maintaining Availability Management Plan in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with DRD 1294CF-008.

b. Addressing end-to-end availability requirements in any designs to ensure compliance with Government design and architecture standards.
c. Addressing end-to-end availability requirements in defining and executing any test plans.
d. Identifying planned downtime and scheduling downtime in collaboration and coordination with Government, I[3]P contractors and other contractors and in accordance with applicable Service Level Agreements.
e. Implementing requested changes to availability metrics and Service Level Agreement in accordance with Government SLM Process.

7.11 IT Service Continuity Management (ITSCM)

7.11.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of ITSCM is to support the overall Business Continuity Management process by ensuring that required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required business timeframes.

Purpose: The purpose of ITSCM is to establish and maintain required ongoing recovery capability within required IT services and their supporting components.

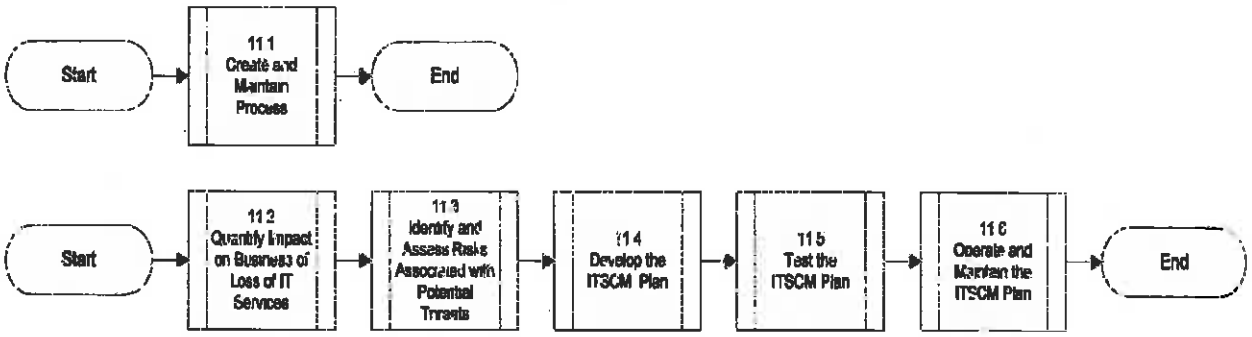

Figure 17: High-Level IT Service Continuity Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing ITSCM Management procedures that align with Government ITSCM Process.
b. Providing ITSCM Services to mitigate the impact of a disaster or major failure in accordance with Government ITSCM Process.
c. Developing, documenting and maintaining procedures (e.g., Disaster Recovery checklists) in collaboration and coordination with Government, I[3]P contractors and other contractors to meet Government requirements (e.g., Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)).

7.11.2 Create and Maintain IT Service Continuity Management Process

The contractor shall be responsible for:

a. Complying with Government ITSCM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government ITSCM process.

7.11.3 Quantify Impact on Business of Loss of IT Services

The contractor shall be responsible for:

a. Providing information to support analysis of the impact of continuity scenarios.
b. Providing information to support identification and impact of contingency options and mitigation actions.

7.11.4 Identify and Assess Risks Associated with Potential Threats

The contractor shall be responsible for:

a. Providing information to support identification of risk responses and proposed countermeasures.
b. Participating in IT risk assessment activities in order to reduce vulnerability to the business.

7.11.5 Develop the IT Service Continuity Management (ITSCM) Plan

The contractor shall be responsible for:

a. Developing and maintaining ITSCM Plan in collaboration and coordination with Government, I^3P contractors and other contractors and in accordance with DRD 1294CF-010.

7.11.6 Test the IT Service Continuity Management (ITSCM) Plan

The contractor shall be responsible for:

a. Developing test scenarios in collaboration and coordination with Government, I^3P contractors and other contractors in support of conducting testing of ITSCM Plan in accordance with Government ITSCM Process.
b. Conducting walkthrough, full, partial and scenario tests in accordance with Government ITSCM Process.

7.11.7 Operate and Maintain the ITSCM Plan

The contractor shall be responsible for:

a. Participating in Government ITSCM reviews in accordance with Government ITSCM Process.
b. Invoking the ITSCM plan in accordance with Government ITSCM Process.
c. Performing training functions including:
    1. Developing and updating the contractor ITSCM training plans and material.
    2. Training the contractor recovery team members.
d. Maintaining local work procedures and contact lists.
e. Performing ITSCM Plan gap analysis and response planning and updating the contractor ITSCM Plan accordingly.
f. Documenting all contingency services provided in Government Service Level Agreements.
g. Executing recovery plans and restoring Service to normal operation.
h. Supporting ITSCM evaluation efforts following disaster events, including providing evaluations and lessons learned and updating the contractor ITSCM Plan as needed.

7.12 Knowledge Management

7.12.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Knowledge Management is to enable organizations to improve the quality of management decision making by ensuring that reliable and secure information and data is available throughout the service lifecycle.

Purpose: The purpose of Knowledge Management is to ensure that the right information is delivered to the appropriate place or person at the right time to enable informed decision making.

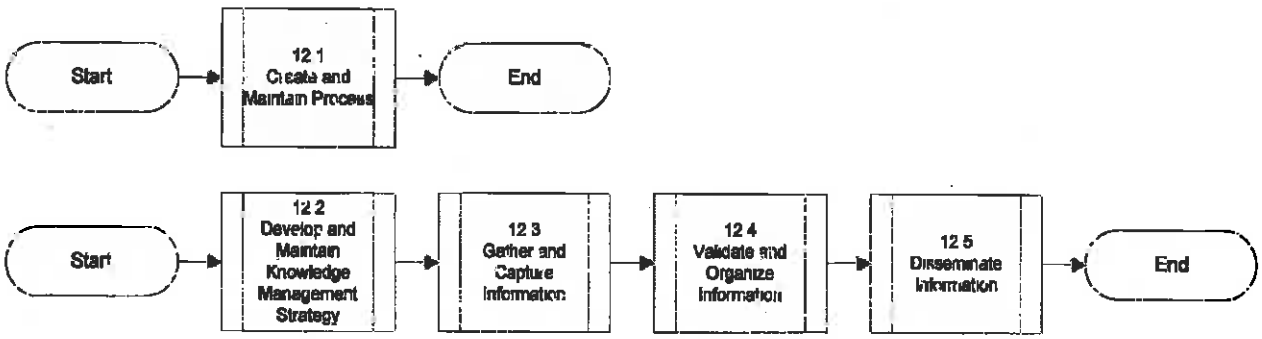

Figure 18: High-Level Knowledge Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

a. Designing and implementing knowledge management procedures and tools to support knowledge capture and dissemination in accordance with Government Knowledge Management Process.

b. Managing and maintaining knowledge and information assets in collaboration and coordination with Government, I³P contractors and other Contractors, and in accordance with Government Knowledge Management Process. This captured developed, generated, and created knowledge and information and related information elements generated as a result of this process shall become the Government Knowledge Base.

7.12.2 Create and Maintain Knowledge Management Process

The contractor shall be responsible for:

a. Complying with Government's Knowledge Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Knowledge Management process.

7.12.3 Develop and Maintain Knowledge Management System

The contractor shall be responsible for providing the Government with information to support develop and maintain of the Government Knowledge Management system.

7.12.4 Gather and Capture Information

The contractor shall be responsible for gathering and capturing information in accordance with Government Knowledge Management Process.

7.12.5 Validate and Organize Information

The contractor shall be responsible for validating and organizing information in accordance with Government Knowledge Management Process.

7.12.6 Disseminate Information

a. The contractor shall be responsible for disseminating information in accordance with Government Knowledge Management Process.
b. The contractor shall make all Knowledge Base information developed, gathered, generated, and or otherwise created under this contract available to the NASA OCIO and ESD in electronic form compliant with the Remedy system requirements and specifications.

7.13 Information Security Management (ISM)

7.13.1 High-Level Process Flow Diagram, Goal and Purpose

Goal: The goal of ISM is to align IT security with business security and ensure that information security is effectively managed across all service management and service delivery activities.

Purpose: The purpose of ISM is to provide a point of focus and management for all aspects of IT security.

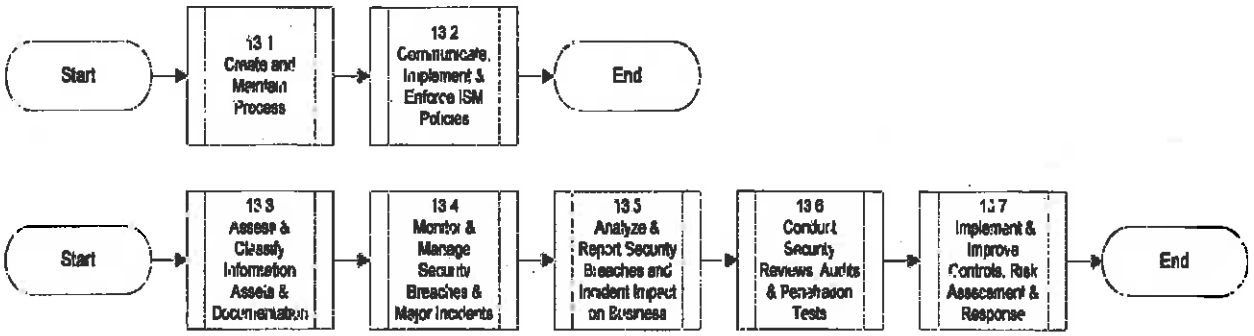

Figure 19: High-Level Information Security Management Process Flow Diagram

7.13.2 Create and Maintain Information Security Management (ISM) Process

The contractor shall be responsible for:

a. Complying with Government's ISM policies and procedures. Examples include Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST). See Section 6, Common Information Technology Security Requirements, in this document.
b. Performing continuous analysis of industry best practices or trends and informing Government of changes that could impact or improve Government ISM process.

7.13.3 Communicate, Implement and Enforce Information Security Management (ISM) Procedures

The contractor shall be responsible for:

a. Implementing Government ISM policies (e.g., FISMA) for all contractor services provided.
b. Supporting Government's ISM policy enforcement efforts and providing details of Information security practices to Government.

7.13.4 Assess and Classify Information Assets and Documentation

The contractor shall be responsible for:

a. Providing information to Government to support information asset identification and documentation in accordance with Government's ISM policy.
b. Providing information to Government to support information asset review activities regarding completeness, accuracy, and vulnerability.
c. Providing information to Government to support classification of information assets in accordance with Government's ISM policy.

7.13.5 Monitor and Manage Security Breaches and Major Incidents

The contractor shall be responsible for:

a. Monitoring and reporting security breaches and security incidents in accordance with Government's ISM procedures.
b. Providing information to Government to support investigation of any security breach and/or security Incident.
c. Providing information to Government to support resolution of any security breach and/or security Incident (DRD 1294CF-012).

7.13.6 Analyze and Report Security Breaches and Incident Impact on Business

The contractor shall be responsible for participating in review and analysis of security breaches and security Incidents and providing detailed information to Government to support analysis of business impact and creation of security breach and security Incident report.

7.13.7 Conduct Security Reviews, Audits and Penetration Tests

The contractor shall be responsible for:

a. Conducting security reviews and regular audits of information and technology assets under Contractor's control in accordance with Government's ISM policy.
b. Participating in periodic Government security audits as requested by Government and coordinating audit activities of Third Parties as required or requested by Government.
c. Conducting and supporting security penetration testing as required or when requested by Government in accordance with Government's ISM policy.

7.13.8 Improve Security Controls, Risk Assessment and Responses

The contractor shall be responsible for:

a. Providing information to Government to support the assessment of security risks.
b. Participating in development and maintenance of security improvement plans in accordance with Government's ISM policy.

8 Common Project Management Guidelines

8.1 Introduction and Overview

I^3P work includes projects that have been approved by the NASA IT governance process to transform elements of the NASA infrastructure. NASA's strategic approach to the management of IT projects is documented in NPR 7120.7, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements*. The contractor shall perform approved projects in compliance with the requirements of the NPR 7120.7 life cycle which includes formulation, implementation, and transition to operation.

8.2 Applicability of NPR 7120.7

The scope of IT projects that are subject to NPR 7120.7 is as follows:

a. The project includes the development of new IT systems or capabilities and is $500K or greater for the total development and implementation cost or affects more than one Center.
b. The project includes the modification to or enhancement of existing IT systems or capabilities and is $500K or greater for the total modification/enhancement cost, regardless of how many Centers are affected.

Some NASA Centers have developed frameworks for the management of projects of smaller scope or size. These frameworks specify a subset of NPR 7120.7 reviews and requirements that are suitable for these smaller projects as determined by the NASA CIO or the CIO of the implementing Center. Such a decision may be made, for example, for reasons related to risk, importance, or visibility of the program or project. For these projects, the Contractor's project and technical management methodology shall ensure compliance with the applicable elements of 7120.7.

9 Glossary of Terms

Activity	A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or plans, and are documented in procedures.
Asset	Any resource or capability. Assets of a contractor include anything that could contribute to the delivery of a service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.
Asset Management	Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process.
Availability	The ability of a CI or IT Service to perform its agreed function when required.
Availability Management	The Process responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT Services. Availability Management is responsible for ensuring that all IT infrastructure, Processes, tools, roles etc are appropriate for the agreed Service Level Targets for availability.
Capacity	The maximum throughput that a CI or IT Service can deliver while meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.
Capacity Management	The Process responsible for ensuring that the capacity of IT Services and the IT infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT Service and plans for short, medium and long term business requirements.
Change	The addition, modification or removal of anything that could have an effect on IT Services. The scope of any Change should include all IT Services, CIs, Processes, documentation etc.
Change Management	The Process responsible for controlling the Lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made with minimum disruption to IT Services.
Component	A general term used to mean one part of something more complex. For example, a computer system may be a Component of an IT Service; an Application may be a Component of a Release unit. Components that are managed as part of an IT Service should be CIs and managed as part of the enterprise Configuration Management Process.

Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people and formal documentation such as Process documentation and SLAs.
Configuration Management	The Process responsible for maintaining information about CIs required to deliver an IT Service, including their relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.
Continual Service Improvement	A stage in the Lifecycle of an IT Service. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services.
Contractor Management	The Process responsible for ensuring that all Contracts with contractors support the needs of the business, and that all contractors meet their contractual commitments.
Customer	Someone who buys goods or services. The Customer of an IT Service contractor is the person or group that defines and agrees the Service Level Targets.
Deployment	The Activity responsible for movement of new or changed hardware, software, documentation, Process, etc., to the live environment. Deployment is part of the Release and Deployment Management Process.
Enterprise Service Desk	The Single Point of Contact (SPOC) between Users and contractors responsible for receiving, logging, escalating, monitoring and closing tickets associated with managing Incidents and Service Requests. Also responsible for communicating with Users regarding the status of Incidents and Service Requests and on-going measurement of Customer satisfaction.
Government	The National Aeronautics and Space Administration (NASA) enterprise along with the collective business units making up the IT Infrastructure and Service delivery environment defined to be in-scope for purposes of the IT Infrastructure Integration Program (I^3P) Acquisition.
Incident	An unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Failure of a CI that has not yet impacted service is also an Incident. For example failure of one disk from a mirror set.
Incident Management	The Process responsible for managing the Lifecycle of all Incidents. The primary objective of Incident Management is to return the IT Service to Users as quickly as possible.

Information Security Management	The Process that ensures the confidentiality, integrity and availability of an organization's assets, information, data and IT Services. Information Security Management usually forms part of an organizational approach to security management which has a wider scope than the IT Service Contractor, and includes handling of paper, building access, phone calls etc., for the entire Organization.
IT Infrastructure	All of the hardware, software, networks, facilities, etc., that are required to develop, test, deliver, monitor, control or support IT Services. The term IT Infrastructure includes all of the information technology but not the associated people, Processes and documentation in support of IT Services.
IT Service	A service provided to one or more Customers by an IT Service Contractor. An IT Service is based on the use of information technology and supports the Customer's business Processes. An IT Service is made up from a combination of people, Processes, and technology and should be defined in a Service Level Agreement.
IT Service Contractor	A Service Provider/Supplier responsible for supplying goods or services that are required to deliver IT Services. These may include commodity hardware and software vendors, network and telecom suppliers and IT outsourcing service providers.
IT Service Continuity Management	The Process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Service contractor can always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and planning for the recovery of IT Services. ITSCM should be designed to support business continuity management.
IT Service Management (ITSM)	The implementation and management of quality IT Services that meet the needs of the business. IT Service Management is performed by contractors in concert with the client enterprise through an appropriate mix of people, Process and information technology.
Knowledge Management	The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an organization. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.
Known Error	A Problem that has a documented root cause and a workaround. Known Errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may be identified by Users, Customers or IT Service Contractors.

Lifecycle	The various stages in the life of an IT Service, CI, Incident, Problem, Change etc. The Lifecycle defines the categories for status and the status transitions that are permitted. For example: • The Lifecycle of an application includes requirements, design, build, deploy, operate, and optimize. • The expanded Incident Lifecycle includes detect, respond, diagnose, repair, recover, restore. • The lifecycle of a server may include: ordered, received, in test, live, disposed etc.
Operational Level Agreement (OLA)	An agreement between an enterprise IT organization and another part of the same organization. An OLA supports the enterprise IT organization's delivery of IT Services to Customers through IT Service Contractors. The OLA defines the goods and services to be provided and the responsibilities of both parties. Performance expectations are documented in SLAs and other Underpinning Contracts.
Performance Work Statement (PWS)	A document containing all requirements for a product purchase, or a new or changed IT Service.
Problem	A cause of one or more Incidents. The cause is not usually known at the time a problem record is created. The Problem Management Process is responsible for further investigation of the Problem.
Problem Management	The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening and to minimize the impact of Incidents that cannot be prevented.
Process	A structured set of Activities designed to accomplish a specific objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A Process may define policies, standards, guidelines, Activities, and work instructions if they are needed.
Recovery Point Objective (RPO)	The maximum amount of data that may be lost when an IT Service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the failure.
Recovery Time Objective (RTO)	The maximum time allowed for recovery of an IT Service following an interruption. Recovery Time Objective is expressed as a length of time from the failure to restoration of the IT Service.
Relationship Manager	Relationship Manager is the person responsible for managing the interaction between the contractor service provider and NASA customers.

Release	A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested and deployed as a single entity.
Release and Deployment Management	The Process responsible for both Release Management and Deployment.
Release Management	The Process responsible for planning, scheduling and controlling the movement of releases to test and live environments. The primary objective of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released. Release Management is part of the Release and Deployment Management Process.
Request For Change (RFC)	A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically.
Request Fulfillment	The Process responsible for managing the Lifecycle of all Service Requests.
Service Asset & Configuration Management	The Process responsible for both Configuration Management and Asset Management.
Service Level	Measured and reported achievement against one or more Service Level Targets.
Service Level Agreement (SLA)	An agreement between a contractor and a Customer. The Service Level Agreement describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service contractor and Customer. A single SLA may cover multiple IT Services or multiple Customers
Service Level Management	The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.
Service Level Targets	Service Level Targets are performance commitments documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements agreed to with the business and ensure IT Service design is aligned with results.

Service Request	A request from a user for information, advice, a standard Change or for access to an IT Service. For example - to reset a password, or to provide standard IT Services for a new user. Service Requests are usually handled by a Service Desk and do not require an RFC (Request For Change) to be submitted.
Single Point of Contact (SPOC)	A designated single, consistent way to communicate with an individual, business entity or enterprise.
Tier 0 (Self Help)	A level of support provided to users via a web-based portal. This Self-Help level of support assists Users resolve lower level of difficulty Incidents and/or Service Requests. The Incidents and/or Service Requests handled at this level of support typically can be resolved through the direct effort of Users, rather than through the effort of resources associated with the Enterprise Service Desk.
Tier 1 Support	The first level in a hierarchy of support groups involved in the resolution of Incidents. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 1 is typically defined as the Enterprise Service Desk (ESD).
Tier 2 Support	The second level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 2 would be the next level of dispatch/escalation from Tier 1 (ESD) support.
Tier 3 Support	The third level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 3 would be the next level of dispatch/escalation from Tier 2 support.
Touch-point	The point or points in the execution of a NASA ITIL process where communication or exchange of information between service providers, customers, and end-users occur.
Underpinning Contract	A Contract between an IT Service contractor and a third party. The third party provides goods or services that support the delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.
Users	A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.

10 Acronym List

ACES	Agency Consolidated End-user Services

APM	Application Portfolio Management
BSMB	Business Systems Management Board
CAB	Change Advisory Board
CF-PWS	Cross-Functional Performance Work Statement
CI	Configuration ItemCI
CIL	Center Integration Lead
CIO	Chief Information Officer
CMDB	Configuration Management Database
CO	Contracting Officer
COTR	Contracting Officer's Technical Representative
CR	Change Request
EA	Enterprise Architecture
EAST	Enterprise Applications Service Technologies
ES&ID	Enterprise Service & Integration Division
ESD	Enterprise Service Desk
ESM	Enterprise Service Management
ESRS	Enterprise Service Request System
FDCCI	Federal Data Center Consolidation Initiative
I^3P	IT Infrastructure Integration Program
ICAM	Identity, Credential, and Access Management
IRM	Information Resources Management
IT	Information Technology
IT PMB	IT Project Management Board
ITIL	IT Infrastructure Library
ITMB	IT Management Board
ITSCM	IT Service Continuity Management
ITSM	IT Service Management
LAN	Local Area Network
MSC	Mission Support Council

NAMS	NASA Access Management System
NCAD	NASA's Consolidated Active Directory
NEAR	NASA EA Repository
NICS	NASA Integrated Communications Services
OCIO	Office of the Chief Information Officer
PDA	Personal Digital Assistant
POC	Point of Contact
PWS	Performance Work Statement
RCA	Root Cause Analysis
RFC	Request for Change
SACM	Service Asset and Configuration Management
SE	Service Executive
SE&I	Systems Engineering & Integration
SIM	Service Integration Management
SLA	Service Level Agreement
SLM	Service Level Management
SLR	Service Level Requirements
SME	Subject Matter Expert
SOIL	Service Office Integration Lead
SOM	Service Office Manager
SPOC	Single Point of Contact
STRAW	System for Tracking and Registering Applications and Websites
TIM	Technical Integration Manager
TRM	Technical Reference Model
WAN	Wide Area Network
WESTPRIME	Web Enterprise Service Technologies

11 Referenced Document List

The following documents are applicable to the cross functional requirements:

a. NASA Enterprise Service Management Concept of Operations
b. NPR 7120.7 NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements
c. NPR 2800.1, Managing Information Technology
d. NPR 2810.1 Security of Information Technology
e. NPR 2830.1 NASA Enterprise Architecture Procedures
f. NPD 1000.0 NASA Strategic Management and Governance Handbook
g. NASA Enterprise Service Desk Concept of Operations
h. NASA Enterprise Service Desk Performance Work Statement
i. NASA Enterprise Architecture Repository (NEAR) Interface Definition Specification (Not valid)
j. Government Availability Management Process
k. Government Capacity Management Process
l. Government Change Management Process
m. Government Incident Management Process
n. Government Information Security Management procedures and policy
o. Government IT Service Continuity Management Process
p. Government Knowledge Management Process
q. Government Problem Management Process
r. Government Release and Deployment Management (RDM) procedures
s. Government Release Plan (part of Government's Release and Deployment Management (RDM) procedures and policy)
t. Government Request Fulfillment Process
u. Government Service Asset and Configuration Management (SACM) Process
v. Government Service Level Management Process
w. Government Supplier Management Process

ATTACHMENT D

IT SECURITY Plan and Management Plan

TBD

ATTACHMENT E

OCI AVOIDANCE PLAN

TBD

ATTACHMENT F

IT SECURITY ADL

01/2012

Information Technology (IT) Security Applicable Documents List
JUNE 2012

NASA Policy Directives (NPD) and NASA Procedural Requirements (NPR)		
Document	**Subject**	**Effective Date**
NPR 1382.1	NASA Privacy Procedural Requirements	August 10, 2007
NPD 1382.17H	NASA Privacy Policy	June 24, 2009
NPD 1440.6H	NASA Records Management	March 24, 2008
NPR 1441.1D	NASA Records Retention Schedules (w/Change 5, 6/29/09)	February 24, 2003
NPD 2540.1G	Personal Use of Government Office Equipment Including Information Technology	June 08, 2010
NPD 2800.1B	Managing Information Technology	March 21, 2008
NPR 2800.1B	Managing Information Technology	March 20, 2009
NPD 2810.1D	NASA Information Security Policy	May 9, 2009
NPR 2810.1A	Security of Information Technology w/ Change 1, May 19, 2011)	May 16, 2006
NPD 2830.1	NASA Enterprise Architecture	December 16, 2005
NPR 2830.1	NASA Enterprise Architecture Procedures	February 9, 2006
NPR 7120.7	NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements	November 3, 2008
NPR 2841.1	Identity, Credential, and Access Management	January 6, 2011

NASA Interim Directive		
Document	**Subject**	**Effective Date**
NM2810-64	NASA Interim Directive: Information Technology Security and Efficiency Requirements	May 22, 2008

NASA Interim Technical Requirements (NITR)		
Document	**Subject**	**Effective Date**
NITR 2800_2	Email Services and Email Forwarding	September 18, 2009
NITR 2800_1	NASA Information Technology Waiver Requirements and Procedures	August 13, 2009
NITR 2830-1B	Networks in NASA Internet Protocol (IP) Space or NASA Physical Space	February 12, 2009
NITR 1382_2	NASA Rules and Consequences to Safeguarding PII, with Change 1, dated 02/04/2008	January 28, 2008

SOPs (ITS-SOP) and Handbooks (ITS-HBK)		
Document	**Subject**	**Effective Date**
ITS-HBK-0002	Roles and Responsibilities Crosswalk	January 3, 2012
ITS-HBK-0201	Security Assessment and Authorization	May 6, 2011
ITS-HBK-0301	Planning	May 6, 2011
ITS-HBK-0401	Risk Assessment	May 6, 2011
ITS-HBK-2810.05-01	Systems and Service Acquisition	November 21, 2011
ITS-HBK-0601	Awareness and Training	May 6, 2011
ITS-HBK-0701	Configuration Management	May 6, 2011
ITS-HBK-0801	Contingency Planning	April 26, 2012
ITS-HBK-0901	Incident Response and Management	May 6, 2011
ITS-HBK-1001	Maintenance	May 6, 2011
ITS-HBK-1101	Media Protection	May 6, 2011
ITS-HBK-1201	Physical and Environmental Protection	May 6, 2011
ITS-HBK-1301	Personnel Security	May 6, 2011

SOPs (ITS-SOP) and Handbooks (ITS-HBK)		
Document	**Subject**	**Effective Date**
ITS-HBK-1401	System and Information Integrity	May 6, 2011
ITS-HBK-1501	Access Control	December 21, 2011
ITS-HBK-1502	Access Control: Elevated Privileges (EP)	January 3, 2012
ITS-HBK-1601	Audit and Accountability	May 6, 2011
ITS-HBK-1701	Identification and Authentication	May 6, 2011
ITS-HBK-1801	System and Communications Protection	May 6, 2011
ITS-HBK 0205	Security Assessment and Authorization: External Information Systems	November 8, 2010
ITS-HBK 0206	Security Assessment and Authorization: Extending and Information Systems Authorization to Operate Process and Templates	November 10, 2010
ITS-HB 0001A	Format and Procedures for an IT Security Handbook	March 29, 2011
ITS-HBK 0207	Security Assessment and Authorization: Information System Security Plan Numbering Schema	November 10, 2010
ITS-HBK 0204	Security Assessment and Authorization: Continuous Monitoring—Annual Security Control Assessments	November 8, 2010
ITS-HBK 0302	Planning: Information System Security Plan Template, Requirements, Guidance and Examples	February 9, 2011
ITS-HBK 0402	Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement	February 11, 2011
ITS-HBK 0202	Security Assessment and Authorization: FIPS 199 Moderate & High Systems	November 10, 2010
ITS-HBK 0203	Security Assessment and Authorization: FIPS 199 Low Systems	November 10, 2010

SOPs (ITS-SOP) and Handbooks (ITS-HBK)		
Document	**Subject**	**Effective Date**
ITS-HBK 0035	Digital Media Sanitization	September 15, 2008
ITS-HBK 0802	Contingency Planning: Guidance and Templates for Plan Development, Maintenance and Test	February 11, 2011
ITS-HBK 0902	NASA Information Security Incident Management	August 24, 2011
ITS-HBK 0903	Targeted Collection of Electronic Data	August 24, 2011

Standards		
Document	**Subject**	**Effective Date**
EA-STD 0001.0	Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorization Infrastructure	August 1, 2008
EA-SOP 0003.0	Procedures for Submitting a NASA Agency Forest (NAF) Deviation Request and Transition Plan	August 1, 2008
EA-SOP 0004.0	Procedures for Submitting an Application Integration Deviation Request and Transition Plan	August 1, 2008
NASA-STD-2804-O	Minimum Interoperability Software Suite	August 9, 2011
NASA-STD-2805-O	Minimum Hardware Configurations	August 9, 2011

Within 30 days after contract award, the Contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer for approval.

ATTACHMENT G

POSITION DESCRIPTIONS

09/07/2012

ATTACHMENT H

PERSONAL IDENTITY VERIFICATION

07/2012

PERSONAL IDENTITY VERIFICATION (PIV) CARD ISSUANCE PROCEDURES

07/20/2012

PIV Card Issuance Procedures in accordance with FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel. FIPS 201 Appendix A graphically displays the following procedure for the issuance of a PIV credential.

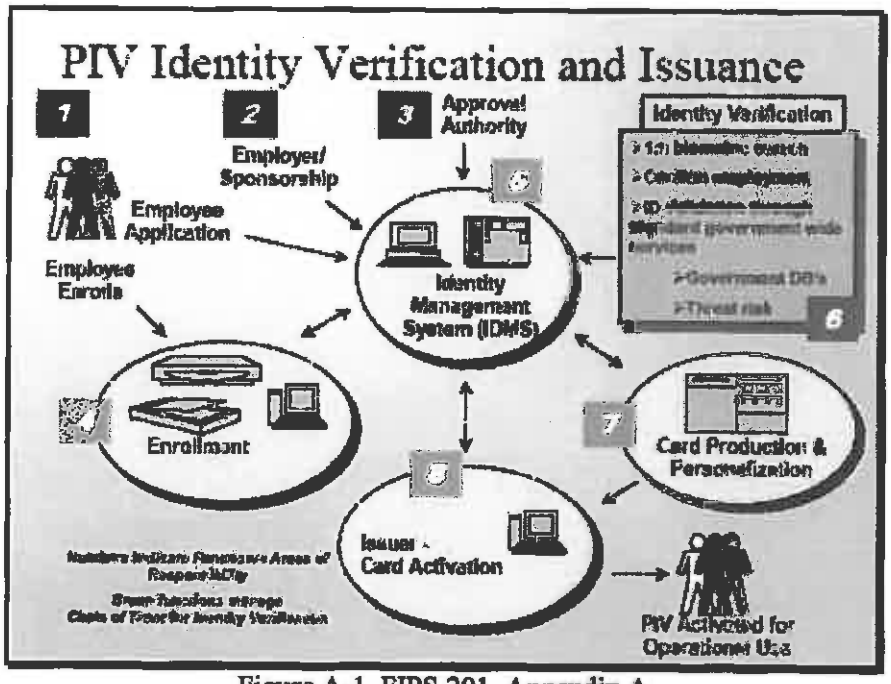

Figure A-1, FIPS 201, Appendix A

The following steps describe the procedures for the NASA Personal Identity Verification Card Issuance (PCI) of a PIV credential:

Step 1:
The Contractor's Corporate Security Officer (CSO), Program Manager (PM), or Facility Security Officer (FSO) submits a formal letter that provides a list of contract employees (applicant) names requesting access to the NASA Contracting Officer's Technical Representative (COTR). In the case of a foreign national applicant, approval through the NASA Foreign National Management System (NFNMS) must be obtained for the visit or assignment before any processing for a PIV credential can take place. Further, if the foreign national is not under a contract where a COTR has been officially designated, the foreign national will provide the information directly to their visit/assignment host, and the host sponsor will fulfill the duties of the COTR mentioned herein. In each case, the letter shall provide notification of the contract or foreign national employee's (hereafter the "applicant") full name (first, middle and last), social security number (SSN) or NASA Foreign National Management System Visitor Number if the foreign national does not

have a SSN, and date of birth. If the contract employee has a current satisfactorily completed National Agency Check with Inquiries (NACI) or an equivalent or higher degree of background investigation, the letter shall indicate the type of investigation, the agency completing the investigation, and date the investigation was completed. Also, the letter must specify the risk/sensitivity level associated with the position in which each applicant will be working (NPR 1600.1, §4.5 is germane) Further, the letter shall also acknowledge that contract employees may be denied access to NASA information or information systems based on an unsatisfactory background investigation/adjudication.

After reviewing the letter for completeness and concurring with the risk/sensitivity levels, the COTR/host must forward the letter to the Center Chief of Security (CCS). The CCS shall review the OPM databases (e.g., DCII, PIP, et al.), and take appropriate steps to validate the applicant's investigation status. Requirements for a NACI or other investigation shall be initiated only if necessary.

Applicants who do not currently possess the required level of background investigation shall be directed to the e-QIP web site to complete the necessary background investigation forms online. The CCS shall provide to the COTR/host information and instructions on how to access the e-QIP for each contract or foreign national employee requiring access

Step 2:
Upon acceptance of the letter/background information, the applicant will be advised that in order to complete the investigative process, he or she must appear in-person before the authorized PIV registrar and submit two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, Employment Eligibility Verification, one which must be a Federal[1] or State issued picture identification. Fingerprints will be taken at this time. The applicant must appear **no later than** the entry on duty date.

When the applicant appears, the registrar will electronically scan the submitted documents; any document that appears invalid will be rejected by the registrar. The registrar will capture electronically both a facial image and fingerprints of the applicant. The information submitted by the applicant will be used to create or update the applicant identity record in the Identity Management System (IDMS).

Step 3:
Upon the applicant's completion of the investigative document, the CCS reviews the information, and resolves discrepancies with the applicant as necessary. When the applicant has appeared in person and completed fingerprints, the package is electronically submitted to initiate the NACI. The CCS includes a request for feedback on the NAC portion of the NACI at the time the request is submitted.

Step 4:

[1] A non-PIV government identification badge, including the NASA Photo Identification Badge, MAY NOT BE USED for the original issuance of a PIV vetted credential

Prior to authorizing physical access of a contractor employee to a federally-controlled facility or access to a Federal information system, the CCS will a National Crime Information Center (NCIC) with an Interstate Identification Index check is/has been performed. In the case of a foreign national, a national check of the Bureau of Immigration and Customs Enforcement (BICE) database will be performed for each applicant. If this process yields negative information, the CCS will immediately notify the COTR/host of the determination regarding access made by the CCS.

Step 5:
Upon receipt of the completed NAC, the CCS will update IDMS from the NAC portion of the NACI and indicate the result of the suitability determination. If an unsatisfactory suitability determination is rendered, the COTR will advise the contractor that the employee is being denied physical access to all federally-controlled facilities and Federal information systems.

Based on a favorable NAC and NCIC/III or BICE check, the CCS will authorize the issuance of a PIV federal credential in the Physical Access Control System (PACS) database. The CCS, based on information provided by the COTR/host, will determine what physical access the applicant should be granted once the PIV issues the credential.

Step 6:
Using the information provided by the applicant during his or her in-person appearance, the PIV card production facility creates and instantiates the approved PIV card for the applicant with an activation date commensurate with the applicant's start date.

Step 7:
The applicant proceeds to the credential issuance facility to begin processing for receipt of his/her federal credential.

The applicant provides to the credential issuing operator proof of identity with documentation that meets the requirements of FIPS 201 (DHS Employment Eligibility Verification (Form I-9) documents. These documents **must** be the same documents submitted for registration.

The credential issuing operator will verify that the facial image, and optionally reference finger print, matches the enrollment data used to produce the card. Upon verification of identity, the operator will locate the employee's record in the PACS database, and modify the record to indicate the PIV card has been issued. The applicant will select a PIN for use with his or her new PIV card. Although root data is inaccessible to the operator, certain fields (hair color, eye color, et al.) may be modified to more accurately record the employee's information.

The applicant proceeds to a kiosk or other workstation to complete activation of the PIV card using the initial PIN entered at card issuance.

ALTERNATIVE FOR APPLICANTS WHO DO NOT HAVE A COMPLETED AND ADJUDICATED NAC AT THE TIME OF ENTRANCE ON DUTY

Steps 1 through 4 shall be accomplished for all applicants in accordance with the process described above. If the applicant is unable to appear in person until the time of entry on duty, or does not, for any other reason, have a completed and adjudicated NAC portion of the NACI at the time of entrance on duty, the following interim procedures shall apply.

1. If the documents required to submit the NACI have not been completed prior to EOD, the applicant will be instructed to complete all remaining requirements for submission of the investigation request. This includes presentation of I-9 documents and completion of fingerprints, if not already accomplished. If the applicant fails to complete these activities as prescribed in NPR 1600.1 (Chapters 3 & 4), it may be considered as failure to meet the conditions required for physical access to a federally-controlled facility or access to a Federal information system, and result in denial of such access.

2. Based on favorable results of the NCIC, the applicant shall be issued a temporary NASA identification card for a period not-to-exceed six months. If at the end of the six month period the NAC results have not been returned, the agency will at that time make a determination if an additional extension will be granted for the temporary identification card.

3. Upon return of the completed NAC, the process will continue from Step 5.

ATTACHMENT I

SAFETY AND HEALTH PLAN

09/07/2012

ATTACHMENT J

DD FORM 254

12/20/2012

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: Top Secret

b. LEVEL OF SAFEGUARDING REQUIRED: Top Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

X	a. PRIME CONTRACT NUMBER: NNH13CH30Z	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		DATE (YYYYMMDD): 20130201
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE (YYYYMMDD)
	c. FINAL *(Complete item 5 in all cases)*		DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Infozen, Inc. 9420 Key West Avenue, Suite 101 Rockville, MD 20850-6379	1QVG9	Defense Security Service 7556 Teague Road, Suite 580 Hanover,MD 21076

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Aquilent 1100 West Street Laurel, MD 20707-3500	3U871	Defense Security Service 7556 Teague Road, Suite 580 Hanover,MD 21076

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Contractor's Facility and NASA Locations	1QVG9	NASA HQ Security Office Office of Security and Program Protection 300 E Street SW, Washington, DC 20546

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Web Enterprise Service Technologies (WEST) PRIME

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)	X	
(2) Non-SCI	X	
f. SPECIAL ACCESS INFORMATION		X
g. NATO INFORMATION		X
h. FOREIGN GOVERNMENT INFORMATION		X
i. LIMITED DISSEMINATION INFORMATION	X	
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)*		X

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X	
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. PERFORM SERVICES ONLY	X	
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
h. REQUIRE A COMSEC ACCOUNT		X
i. HAVE TEMPEST REQUIREMENTS		X
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
l. OTHER *(Specify)* See Item 13.	X	

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*

The NASA HQ Security Classification Officer and to the Officer of Public Affairs, NASA HQ, Washington, DC 20546

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

A. Classification of Materials will be handled in accordance with the following references:
- NPR 1600.1 NASA Security Procedures and Guidelines
- NPR 1620.3 Physical Security Requirements for NASA Facilities and Property
- NPD 2800.1B Managing Information Technology
- NPR 2800.1 Managing Information Technology
- NDP 2810.1C NASA Information Technology
- NPR 2810.1A Security Information Technology
- Department of Defense (DOD 5220.22M) National Industrial Security Program Operating Manual

B. Contractor's normal access to classified will be at: NASA HQ's 300 E. Street Washington, DC. 20546
Classified information will normally be stored at NASA HQ's.
C. Security clearance verifications will be process through NASA Security
D. All classified work shall be performed on NASA facilities, or as directed by the Government. No secure information will be retained at Contractor or Sub-Contractor facilities.
E. SCI Security Guidance
-- DCI Directive 6/1 Security Policy for SCI and Security Policy Manual
-- Intelligence Community (IC) Policy Memo (ICPM) 2006-700-6 amends DCID 6.1. Access to SCI and other Controlled Access program Information and associated IC Policy Guidance 704.1 thru 704-3.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] Yes [ ] No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

Federal Risk and Authorization Management Program (FedRAMP)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [ ] Yes [X] No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Joe Costanza	Deputy Chief of Security	(202) 358-2279

d. ADDRESS *(Include Zip Code)*	e. SIGNATURE
NASA HQ Security Office Office of Security and Program Protection 300 E Street SW, Washington, DC 20546	

17. REQUIRED DISTRIBUTION

[X]	a. CONTRACTOR
[ ]	b. SUBCONTRACTOR
[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
[ ]	f. OTHERS AS NECESSARY