

contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(j) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(k) Paragraphs (d) and (f) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

AkinsCrisp Public Strategies, 116 Jefferson Street, Suite #305, Huntsville, AL 35801
AI Signal Research, Inc. (ASRI), 3411 Triana Blvd., SW, Huntsville, AL 35805

(End of Clause)

I.10 1852.204-76 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (NOVEMBER 2004) (DEVIATION)

(a) The Contractor shall be responsible for information and information technology (IT) security when the Contractor or its subcontractors must obtain physical or electronic (i.e., authentication level 2 and above as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure, or where information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, is stored, generated, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

(b) IT Security Requirements.

(1) Within 45 days after contract award, a Contractor shall submit to the Contracting Officer for NASA approval an IT Security Plan, Risk Assessment, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Assessment. These plans and assessments, including annual updates shall be incorporated into the contract as compliance documents.

(i) The IT system security plan shall be prepared consistent, in form and content, with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, and any additions/augmentations described in NASA Procedural Requirements (NPR) 2810, Security of Information Technology. The security plan shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of Federal Information Processing Standards (FIPS) 200, Recommended Security Controls for Federal Information Systems. The plan shall be reviewed and updated in accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and FIPS 200, on a yearly basis.

(ii) The risk assessment shall be prepared consistent, in form and content, with NIST SP 800-30, Risk Management Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The risk assessment shall be updated on a yearly basis.

(iii) The FIPS 199 assessment shall identify all information types as well as the "high water mark," as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.

(2) The Contractor shall produce contingency plans consistent, in form and content, with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The Contractor shall perform yearly "Classroom Exercises." "Functional Exercises," shall be coordinated with the Center CIOs and be conducted

NNM07AA70C

once every three years, with the first conducted within the first two years of contract award. These exercises are defined and described in NIST SP 800-34.

(3) The Contractor shall ensure coordination of its incident response team with the NASA Incident Response Center and the NASA Security Operations Center.

(4) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPR 2810 requirements. The Contractor may use web-based training available from NASA to meet this requirement.

(5) The Contractor shall provide NASA, including the NASA Office of Inspector General, 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 IT security inspection, investigation, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA information or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime. To facilitate mandatory reviews, the Contractor shall ensure appropriate compartmentalization of NASA information, stored and/or processed, either by information systems in direct support of the contract or that are incidental to the contract.

(6) 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, demonstrate knowledge appropriate to those tasks. Knowledge is demonstrated through the NASA System Administrator Security Certification Program. A system administrator is one who provides IT services, network services, files storage, and/or web services, to someone else other than themselves and takes or assumes the responsibility for the security and administrative controls of that service. Within 30 days after contract award, the Contractor shall provide to the Contracting Officer a list of all system administrator positions and personnel filling those positions, along with a schedule that ensures certification of all personnel within 90 days after contract award. Additionally, the Contractor should report all personnel changes which impact system administrator positions within 5 days of the personnel change and ensure these individuals obtain System Administrator certification within 90 days after the change.

(7) When the Contractor is located at a NASA Center or installation or is using NASA IP address space, the Contractor shall --

(i) Submit requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the Network Security Configuration Control Board (NSCCB);

(ii) Comply with the NASA CIO metrics including patch management, operating systems and application configuration guidelines, vulnerability scanning, incident reporting, system administrator certification, and security training; and

(iii) Utilize the NASA Public Key Infrastructure (PKI) for all encrypted communication or non-repudiation requirements within NASA when secure email capability is required.

(c) Physical and Logical Access Requirements.

(1) Contractor personnel requiring access to IT systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPR 2810 and Chapter 4, NPR 1600.1, NASA Security Program Procedural Requirements. NASA shall provide screening, appropriate to the highest risk level, of the IT systems and information accessed, using, as a minimum, National Agency Check with Inquiries (NACI). The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of NASA, interim access may be granted pending completion of the required investigation and final access determination. For Contractors who will reside on a NASA Center or installation, the security screening required for all required access (e.g., installation, facility, IT, information, etc.) is consolidated to ensure only one investigation is conducted based on the highest risk level. Contractors not residing on a NASA installation will be screened based on their IT access risk level determination only. See NPR 1600.1, Chapter 4.

NNM07AA70C

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT-1 has the highest level of risk).

(i) IT-1 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT-2 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of "level 1" information whose cost to replace exceeds one million dollars.

(iii) IT-3 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the Contractor for NASA whose function or information has substantial cost to replace, even if these systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as established in Chapter 4, NPR 1600.1.

(4) The Contractor may conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate to the Contracting Officer that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures for the risk level assigned for the IT position.

(5) Subject to approval of the Contracting Officer, the Contractor may forgo screening of Contractor personnel for those individuals who have proof of a --

(i) Current or recent national security clearances (within last three years);

(ii) Screening conducted by NASA within the last three years that meets or exceeds the screening requirements of the IT position; or

(iii) Screening conducted by the Contractor, within the last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer and concurred on by the CCS.

(d) The Contracting Officer may waive the requirements of paragraphs (b) and (c)(1) through (c)(3) upon request of the Contractor. The Contractor shall provide all relevant information requested by the Contracting Officer to support the waiver request.

(e) The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

(f) The Contractor shall insert this clause, including this paragraph (f), in all subcontracts when the subcontractor is required to --

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(End of Clause)

I.11 OMBUDSMAN (NFS 1852.215-84) (OCT 2003) (Alternate I) (Jun 2000)

(a) An ombudsman has been appointed to hear and facilitate the resolution of concerns from Offerors, potential Offerors, and contractors during the pre-award and post-award 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 Committee, 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, Ms. Robin N. Henderson, George C. Marshall Space Flight Center, DE01, Building 4200, Marshall Space Flight Center, AL 35812, telephone: 256-544-1919, facsimile: 256-544-7920, and e-mail address: Robin.N.Henderson@nasa.gov.

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, e-mail, james.a.balinskas@nasa.gov. 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 elsewhere in this document.

(End of Clause)

I.12 MINIMUM INSURANCE COVERAGE (NFS 1852.228-75) (OCT 1988)

The Contractor shall obtain and maintain insurance coverage as follows for the performance of this contract:

(a) Worker's compensation and employer's liability insurance as required by applicable Federal and state workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with the Contractor's commercial operations that it would not be practical. The employer's liability coverage shall be at least \$100,000, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

(b) Comprehensive general (bodily injury) liability insurance of at least \$500,000 per occurrence.

(c) Motor vehicle liability insurance written on the comprehensive form of policy which provides for bodily injury and property damage liability covering the operation of all motor vehicles used in connection with performing the contract. Policies covering motor vehicles operated in the United States shall provide coverage of at least \$200,000 per person and \$500,000 per occurrence for bodily injury liability and \$20,000 per occurrence for property damage. The amount of liability coverage on other policies shall be commensurate with any legal requirements of the locality and sufficient to meet normal and customary claims.

(d) Comprehensive general and motor vehicle liability policies shall contain a provision worded as follows:

"The insurance company waives any right of subrogation against the United States of America which may arise by reason of any payment under the policy."

(e) When aircraft are used in connection with performing the contract, aircraft public and passenger liability insurance of at least \$200,000 per person and \$500,000 per occurrence for bodily injury, other than passenger liability, and \$200,000 per occurrence for property damage. Coverage for passenger liability bodily injury shall be at least \$200,000 multiplied by the number of seats or passengers, whichever is greater.

(End of Clause)

I.13 RELEASE OF SENSITIVE INFORMATION

(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) 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 [insert page numbers or other identification of pages].

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

NNM07AA70C

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.

NNM07AA70C

(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.

(h) The Contractor shall comply with all requirements of DRD1140-MA-007, Organizational Conflict of Interest (OCI) Avoidance Plan.

(End of clause)

I. 14 ACCESS TO SENSITIVE INFORMATION (NFS 1852.237-72) (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.

NNM07AA70C

(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)

I.15 REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR QUOTERS INCORPORATED BY REFERENCE (MSFC 52.252-90) (FEB 2001)

The Representations, Certifications, and Other Statements of Offerors or Quoters (Section K of the solicitation document) as completed by the Contractor are hereby incorporated in their entirety by reference, with the same force and effect as if they were given in full text.

(End of Clause)

[END OF SECTION]

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

<u>Attachment No.</u>	<u>Description</u>	<u>Pages</u>
J-1	Performance Work Statement (PWS)	J-1-1 – J-1-21
J-2	Performance Requirements (PRS) Summary	J-2-1 – J-2-4
J-3	Surveillance and Cost Plus Incentive Fee Plan	J-3-1 – J-3-12
J-4	Work Breakdown Structure (WBS)	J-4-1
J-5	Schedule of Fully Burdened Not-to-Exceed IDIQ Labor Rates for the Prime Contractor	J-5-1
J-6	Personal Identity Verification (PIV) Procedures	J-6-1 – J-6-4
J-7	Installation-Provided Property and Services	J-7-1 – J-7-11
J-8	IDIQ Task Order Process Flow Chart	J-8-1
J-9	Safety, Health and Environmental Plan	J-9-1
J-10	Safety & Health Management Implementation Guide and Assessment Matrix	J-10-1 – J-10-3
J-11	Strategic Communication Process	J-11-1
J-12	(Reserved)	N/A
J-13	Data Procurement Document (DPD)	J-13-1 – J-13-28
J-14	Work Management / Work Order Process	J-14-1
J-15	(Reserved)	N/A
J-16	(Reserved)	N/A
J-17	IDIQ Labor Category Position Descriptions	J-17-1 – J-17-2
J-18	Wage Determination	J-18-1 – J-18-9
J-19	Applicable Regulations, Procedures, and Documents	J-19-1 – J-19-3
J-20	Acronym List	J-20-1 – J-20-3

ATTACHMENT J-1

PERFORMANCE WORK STATEMENT (PWS)

- 1.0 Scope
- 2.0 OSAC Mission
- 3.0 Program Management
 - 3.1 Contract Management
 - 3.2 Property Management
 - 3.3 Occupational Safety and Health
 - 3.4 Work Management
 - 3.5 Data Collection
 - 3.6 Information Technology Security
- 4.0 Strategic Research & Analysis
 - 4.1 Environmental Monitoring
 - 4.2 Stakeholder Analysis
 - 4.3 Audience Research
 - 4.4 Measuring Communication Effectiveness
 - 4.5 Benchmarking
- 5.0 Communication Strategy, Planning and Message Management
 - 5.1 Communication Goals & Strategy
 - 5.2 Communication Plans
 - 5.3 Key Message Development and Management
 - 5.4 Channel Relationship Development
- 6.0 Communication Services and Product Development / Delivery
 - 6.1 Center Collateral Development
 - 6.2 Executive Communications
 - 6.3 Employee Communications
 - 6.4 Public Inquiry Responses
 - 6.5 Media Products
 - 6.6 Web Content Management
 - 6.7 Technical Documents and Products
 - 6.8 Exhibits
 - 6.9 Events
- 7.0 Indefinite Delivery/Indefinite Quantity

1.0 Scope

The scope of this Performance Work Statement (PWS) provides comprehensive communications services to support the Office of Strategic Analysis and Communications (OSAC) in achieving the communication goals and strategies of NASA and Marshall Space Flight Center (Marshall). To that end, OSAC will execute an overarching communication strategy that includes clearly and consistently communicating NASA's strategic vision and guidance, and Marshall's direction, roles, capabilities, and expectations – internally and externally – to various stakeholder groups. In accomplishing these communication activities that directly support the advancement of Agency goals and Marshall mission assignments, the contractor shall provide communications related support as outlined below.

The contractor shall support Marshall in implementing and maintaining a strategic communications capability that integrates and aligns the Center's communications with Agency direction to enable informed communications and manage effective stakeholder relationships for advancement of NASA's strategic goals. The communications capability shall consist of three primary, integrated functional areas: strategic research & analysis; communication strategy, planning and message management; and communication services and product development/delivery.

Strategic research & analysis, as described in PWS 4.0, shall serve as the foundation for communications by infusing research and analysis results into the development of strategy and planning consistent with Agency direction; message management aligned with NASA's key messages; and communication services and products required by the Center and its assigned programs and projects. Communication strategy, planning and message management, as described in PWS 5.0, shall serve as a major cohesive element and drives all communication service and product development activities. Communication services and product development / delivery, as described in PWS 6.0, shall provide vehicles and venues for communications with NASA and Marshall's stakeholders. A visual representation of this communication process is included in Attachment J-11.

In performing the requirements of the PWS, the contractor shall clearly demonstrate an understanding of the difference between communications and strategic communication as an integrative process guiding strategy and messaging through audience-driven delivery mechanisms. The contractor shall ensure that communications are based on a clear understanding of the targeted audience and convey NASA direction and guidance and Marshall's role and responsibilities in accomplishing the Agency's missions. Messages must be designed to reach and connect with the desired audience in a compelling format, and the right mix of channels must be selected to obtain the desired exposure and outcomes. The contractor shall measure communication results and incorporate refinements into future communication strategies.

In order to establish successful communication capabilities, the contractor shall develop, implement, and execute a comprehensive suite of services, products, tools, and techniques across all functional and sub-functional elements within the PWS.

The contractor shall support OSAC management and OSAC's customers in a responsive, integrated, and communicative manner. The contractor shall work as a team with OSAC to contribute to the organization's success. The contractor shall demonstrate an understanding of OSAC's communication mission and act as a member of an integrated OSAC team in providing new and innovative communication services.

2.0 OSAC's Communication Mission

Consistent with Agency direction and guidance, OSAC, as Marshall's organization chartered to develop and manage the Center's communications system, is responsible for creating, preserving, and strengthening support for NASA's vision and missions, and ensuring that analysis and communications are integrated and aligned with NASA direction and guidance and Marshall mission assignments. OSAC's Organizational Chart, Attachment L-7, shows communication functions and performance management functions as outlined below:

Communication Management:

OSAC's communication mission is to develop, execute and guide a strategic communications capability to manage stakeholder relationships based on agency direction, program intelligence, and center strategies and priorities. OSAC will fulfill its mission by:

- Building a communication system (people, processes, tools) that is recognized within Marshall as the preferred provider of communication strategy, products and services and as a critical capability to enable Marshall's future
- Enabling message-sharing and exchange to promote an accurate and positive representation of Marshall throughout NASA and the external community with communication products and services
- Increasing the Center workforce's knowledge about NASA direction and guidance and Marshall's goals and objectives in fulfilling the Center's assignments
- Promoting inter-organizational information-sharing across the Center and with key stakeholders
- Supporting accountability for communication within the Center's workforce
- Fostering two-way communication throughout the Center

The infusion of communications into daily activities is essential for organizational health and sustainability. OSAC's mission approach is customer-driven, results-oriented and multi-faceted. OSAC is committed to helping Marshall achieve success through efficient, responsive and timely planning and execution of a continuum of communications products and services.

Performance Management:

OSAC's overall mission also includes the Center's performance management function. This function provides integrated analysis, planning, and evaluation of Marshall's program, project, and institutional performance relative to Agency direction and guidance and Marshall's mission assignments. Performance Management efforts are not included in this PWS.

3.0 Program Management

The contractor shall provide administration and technical management for effective direction, control, and integration of all efforts performed under this contract. This includes the development and execution of a disciplined management philosophy and clearly defined processes and tools to be applied and integrated throughout contract activities to meet all requirements of the performance work statement. The contractor shall provide a system to measure and monitor contract performance on all PWS activities. Additionally, the contractor shall be required to travel in support of various PWS activities.

The contractor shall report and document this work and fulfill the requirements of associated Data Requirement Descriptions (DRD's) as outlined in Data Procurement Document (DPD) 1140 (Attachment J-13). The contractor shall determine the data restriction that applies to each data deliverable and mark or transmit the data restriction in accordance with section 2.3.3 of the Data Procurement Document.

In performing the effort delineated in this PWS, the contractor shall provide systems and applications associated with the six covered Electronic and Information Technology Accessibility product groups specified below. All systems and applications associated with these groups shall comply with the applicable standards contained with the Federal Acquisition Circular 97-27, Electronic and Information Technology (EIT) Accessibility, Section 508 of the Rehabilitation Act of 1973 by implementing the applicable Technical Standards (Subpart B) including:

- 1) Software Applications and Operating Systems (1194.21)
- 2) Web-based Intranet and Internet Information and Applications (1194.22)
- 3) Telecommunications Products (1194.23)
- 4) Video or Multimedia Products (1194.24)
- 5) Self-Contained Closed Products (1994.25)
- 6) Desktop and Portable Computers (1194.26)

The contractor shall comply with the requirements of the Americans with Disabilities Act.

3.1 Contract Management. The contractor shall provide planning, integration, and management of all contract activities to ensure disciplined and quality performance of work and timely application of resources necessary for work completion. Contract management effort shall apply to the entire performance work statement (PWS); including, the mission schedule and all Indefinite Delivery/Indefinite Quantity (IDIQ) task orders issued by Marshall.

The contractor's plan and approach for contract administration and technical management shall be documented and submitted in a Management Plan in accordance with DRD 1140MA-001. The contractor shall clearly document in the Management Plan the integrated processes by which the PWS will be performed. The contractor shall provide and use an integrated management system to monitor and measure performance of planning, scheduling, progress reporting, quality assurance, and completion of work orders or projects. This shall include an automated electronic work order management system for life cycle management of all work orders and shall include the capability to provide real-time current and historical status of all work orders from initiation to completion.

In support of the contractor's management approach, the contractor shall prepare and submit the following: Financial Management Report (533M and 533Q) in accordance with DRD 1140MA-002; Quarterly and Monthly Technical Progress Reports in accordance with DRD 1140MA-003; Badged Employee and Remote IT User Listings in accordance with DRD 1140MA-004; Contractor Employee Clearance Documents in accordance with DRD 1140MA-005; Position Risk

NNM07AA70C

Designation for Non-NASA Employee Forms in accordance with DRD 1140MA-006; and Organizational Conflict of Interest (OCI) Avoidance Plan in accordance with DRD 1140MA-007.

3.2 Property Management. The contractor shall implement an inventory control system for all controlled property and equipment. The contractor shall prepare and maintain a database identifying and listing all equipment, materials, tools, etc., provided by the Government for use by the contractor in the performance of contracted effort, and for which the contractor has been given physical custody. The Government Property Management Plan shall be prepared and maintained in accordance with DRD 1140LS-001.

The contractor shall comply with the following specifications and government work instructions:

MWI 4220.1	Space Utilization, Communications Furniture, Relocation, and Special Event Services
MWI 4200.1	Equipment Control
MWI 4300.1	Disposal Turn-Ins / Reutilization Screening
MWI 4500.1	Property Support: Furniture Operations, Retail Supply Operations, Warehousing, and Food Services
MWI 4520.1	Receiving
MWI 4520.2	Use of Procurement Discrepancy Tracking System (PDTS)
MPR 4000.2	Property Management
FAR Part 45	Government Property
NFS Part 1845	Government Property

3.3 Occupational Safety and Health. The Contractor shall establish and implement an industrial/occupational safety, health, and environmental program and provide a Safety, Health, and Environmental (SHE) Plan in accordance with DRD 1140SA-001. The contractor's industrial/occupational safety, health, and environmental program shall incorporate the following:

- a. Management leadership and employee involvement.
- b. System and worksite analysis.
- c. Hazard prevention and control.
- d. Safety and health training.
- e. Environmental compliance.

The contractor shall report mishaps and safety statistics to the Marshall S&MA Office in accordance with DRD 1140SA-002.

The contractor shall provide building managers and safety monitors for buildings 4466, 4631, and 7214. For these buildings, the contractor shall perform required surveys and reports on chemical inventories and warehouse space requirements.

The contractor shall place special emphasize on safety procedures for all exhibit operations, especially as it relates to the use of hazardous/controlled chemicals, fabrication and heavy equipment usage, transportation, and public safety in all venues, etc.

3.4 Work Management. The contractor shall establish, implement, and maintain an automated electronic work order system required to plan, organize, direct, and control contract activities for materials, supplies, equipment and travel associated with the core mission portion and IDIQ Task Orders. The work order system shall reflect technical and budget content in support of OSAC and OSAC's customers (including Marshall's Engineering Directorate, Shuttle Propulsion Office, Exploration Launch Office, Science & Missions Systems Office and NASA

Headquarters Exploration Systems Management Directorate and Public Affairs Office). The contractor shall provide the Government with access to the automated electronic work order management system as depicted in Attachment J-14. The automated electronic system shall be an interactive system to be used by the government and the contractor. The automated electronic system shall provide electronic routing and approval of work orders (WOs) to authorized government and contractor approving officials. In addition, the contractor's automated system shall track the status of each WO from planning/initiation to completion and record projected and actual resources data for each. This data shall be reported by unique project numbers (UPN) and have direct tracking capability to the estimated and actual costs back in the contractor's Financial Management Report (per DRD 1140MA-002) at all levels down to WO cost sub-elements and organizational funding levels. The contractor's automated electronic system shall be an integrated system that allows insight and management of the PWS requirements.

The contractor's automated electronic work order management system shall provide a unique project numbering system with traceability of tasks through their lifetime; electronic notification of the order's status; approval tracking, revision tracking, traceability to a minimum of PWS level 3, delineation of inactive and active tasks, period of performance of each task, and estimated and actual costs. The system shall be capable of allowing the COTR, Performance Monitors, and Contractor Program Manager the ability to review and approve each work order prior to beginning the task.

Each Work Order shall include: a WO number allowing traceability to OSAC or the requesting organization; traceability to a minimum of PWS level 3; name of the government requesting official; work order initiator; work order description and/or objectives; total estimated and actual costs by major cost element, as applicable (such as materials, supplies, equipment and travel, etc.); deliverables and milestone dates; benefiting program(s); and special instructions.

The automated electronic work order system shall be capable of providing a Cost Summary Report, in spreadsheet form, that contains the following information for the base year and each option year for each organization/customer: WO number; WO title; total estimated and actual costs with and without fee. The Cost Summary Report shall roll-up each PWS level 3 elements into an overall contract performance summary. Additionally, the system shall allow query capability by each UPN element and work order number. The contractor shall submit a monthly work order report in accordance with DRD 1140MA-003, Quarterly and Monthly Technical Progress Reports.

3.5 Data Collection. The contractor shall develop and maintain an integrated, electronic data collection system to capture and store information and content for PWS functional sub-elements. The automated electronic system shall be an interactive system to be used by the government and the contractor. The electronic system shall provide data cross-referencing capability across PWS functional sub-elements to inform and assist in the execution of all strategic communication contract activities. Additionally, the contractor shall provide a relational electronic archive of all final products and plans delivered and accepted by OSAC for version control and reference. The contractor shall provide and maintain a comprehensive matrix of all databases and systems to be implemented in support of the PWS data control measures. The contractor shall identify administrative POC's, data / information captured by functional sub-element, accessibility requirements, and integration capabilities.

3.6 Information Technology Security. The contractor shall prepare a Contract Information Technology Security Program Plan (CITSPP) that documents how the contractor and subcontractor personnel will comply with the requirements of NPR 2810.1, Security of Information Technology. The contractor's CITSPP shall address security measures for any systems and