



Attachment J-1
Performance Work Statement (PWS)

For

Enterprise Applications Service
Technologies (EAST) 2

ATTACHMENT J-1

Table of Contents

1 ENTERPRISE APPLICATIONS SERVICE TECHNOLOGIES (EAST) 2.....3

1.1 MISSION STATEMENT3

1.2 GOALS AND OBJECTIVES4

1.3 GOVERNMENT RETAINED AUTHORITIES5

1.4 GENERAL DESCRIPTION OF WORK REQUIREMENTS.....5

2 PROGRAM MANAGEMENT.....6

2.1 CONTRACT MANAGEMENT6

2.2 FINANCIAL MANAGEMENT7

2.3 PROCUREMENT MANAGEMENT8

2.4 PROGRAM SUPPORT9

2.5 SECURITY MANAGEMENT10

2.6 SAFETY, HEALTH AND ENVIRONMENTAL (SHE) REQUIREMENTS12

3 APPLICATIONS OPERATIONS13

3.1 APPLICATIONS MAINTENANCE.....14

3.2 APPLICATIONS ENHANCEMENT.....17

4 IDIQ OPTIONAL SUPPORT FOR NASA CENTER-SPECIFIC APPLICATIONS.18

5 DELIVERY FUNCTIONS20

5.1 OPERATIONS MANAGEMENT20

5.2 APPLICATION FUNCTIONAL SUPPORT25

5.3 APPLICATION DEVELOPMENT26

5.4 APPLICATION TECHNICAL OPERATIONS & MAINTENANCE (ATOM)..27

5.5 INFORMATION ASSURANCE.....29

5.6 CROSS FUNCTIONAL INTEGRATION35

ATTACHMENT J-1

1 ENTERPRISE APPLICATIONS SERVICE TECHNOLOGIES (EAST) 2**1.1 MISSION STATEMENT**

Since its establishment, the National Aeronautics and Space Administration (NASA) (also referred to as the Government or the Agency) has continued to evolve as a result of changing missions and priorities. Similarly, NASA's Information Technology (IT) infrastructure is evolving toward a level of maturity that will allow it to successfully change NASA's existing IT environment into a seamless and truly integrated IT architecture. NASA recognizes that effectively and efficiently creating, researching, managing, preserving, protecting, and disseminating the information required to achieve the objectives of space exploration, as well as other NASA missions, is vital to its mission success.

The nature of NASA's program implementation model requires extensive cross-Center collaboration which is vital to the planning, design, and development of mission-related capabilities and technology in the future. Therefore, NASA requires a seamless technical IT infrastructure to ensure interoperability both within programs and across Centers and facilities.

As the world leader in aeronautics, space exploration, and scientific research, NASA considers its Applications vital to its continued success. NASA personnel use IT to support NASA's core business, scientific, research, and computational activities. It is imperative that the commercial sector delivers secure and cost-effective IT services that meet NASA's mission and program needs while achieving efficiency and high level customer satisfaction.

Within this framework, the task of the EAST 2 Contractor (hereafter referred to as the Contractor) is to provide, manage, secure, and maintain IT services that meet the requirements as defined in this Performance Work Statement (PWS).

The primary purpose of the EAST 2 contract is to provide all services necessary to operate the NASA Enterprise Applications Competency Center (NEACC). The NEACC provides services to operate, maintain, and enhance key Business and Mission-Supporting platforms, applications and infrastructure used across the Agency. With the expanded scope to include MSFC Center-specific Application delivery services and to optionally incorporate other NASA Center-specific applications, NEACC refers to both Enterprise and Center-specific applications under EAST 2.

The EAST 2 scope will provide a contractual vehicle for other NASA Centers to optionally utilize support in the future for their Center's unique applications as required. Potential Centers that are considered to be in-scope and may be included in the future under the EAST 2 contract include the following NASA locations:

- Ames Research Center, CA

ATTACHMENT J-1

- Armstrong Flight Research Center, CA
- Glenn Research Center, OH
- Goddard Space Flight Center, MD
- Johnson Space Center, TX
- Kennedy Space Center, FL
- Langley Research Center, VA
- NASA Headquarters, Washington D.C.
- NASA Shared Services Center, MS
- Stennis Space Center, MS
- Associated Center facilities (e.g., Michoud Assembly Facility, Wallops Flight Facility, and White Sands Test Facility etc.)

As NASA focuses its attention on the successful accomplishment of its core mission objectives, it is imperative that all Applications operate reliably and effectively. In addition, it is important that Applications Services—as supporting functions—are offered to the Agency at the best possible value.

1.2 GOALS AND OBJECTIVES

The NASA Chief Information Officer (CIO) has established the following principles to guide tactical decisions and planning:

- **Mission-Enabling:** NASA's IT and IT processes must be mission-enabling, customer-focused, mobile, and interoperable, supporting near-term and longer-term customer needs, and serving as a key enabler for achieving NASA's missions and programs.
- **Purposeful:** IT capabilities continue to rapidly evolve globally. NASA will make smart, value-added innovation and investment in enterprise IT in order to shape its future by optimizing the return on limited resources and serve as a force multiplier for mission accomplishment.
- **Responsive:** The design and operations of NASA's IT must ensure scalability and accountability in order to responsively accommodate mission needs, IT requirements, and business conditions as they unfold.
- **Secure:** Information security is critical to mission integrity and the protection of national assets. NASA IT will proactively and efficiently manage information security and privacy to reduce risk to mission success and to enable innovation.
- **Integrated:** NASA IT must operate as an integrated team of groups aligned by shared goals to effectively support NASA's missions and partners. IT customers and partners will be included appropriately throughout NASA's IT life cycle across IT planning, execution and evaluation.
- **Cost-Effective:** Maximizing value from limited resources is achieved through balanced near- and long-term portfolio decision-making guided by NASA's goals. NASA IT strives to provide efficient services today while evolving an effective enterprise architecture discipline that affordably sustains NASA's IT needs for tomorrow.

ATTACHMENT J-1

In support of these key principles and the Agency's goals as identified in the 2014 NASA Information Resources Management (IRM) Strategic Plan, the following goals are established for the EAST 2 contract:

1. Serve as effective partners with NASA Centers, programs and projects throughout the project development and operations lifecycle such that the Agency's IT investments are optimized, agile, and responsive to customer needs.
2. Optimize the use of standardized IT solutions that meet Agency and Center needs; improve IT security posture; eliminate redundancies; and meet external stakeholder mandates.
3. Achieve development and operations efficiencies by utilizing common processes and infrastructure across the NEACC-managed Enterprise and Center application lifecycle.
4. Work with other Service Areas to develop an integrated architecture that supports the Agency's IT strategy and Enterprise Architecture.
5. Continually assess NASA's IT architecture to identify opportunities for new technology and process insertions that improve efficiency/capabilities; increase agility; reduce cost; and better enable NASA's mission.

1.3 GOVERNMENT RETAINED AUTHORITIES

The Government will retain a set of key authorities that encompass the overall service strategy and service design related to Enterprise and Center-specific Applications services. The Government will also retain authority for all demand management, governance, and approval functions associated with the NEACC and the EAST 2 Contract.

1.4 GENERAL DESCRIPTION OF WORK REQUIREMENTS

The EAST 2 PWS describes comprehensive services for operations, maintenance, enhancement and end-user support for Enterprise and Center-specific Applications. To accomplish this core mission, it will be necessary to apply a systematic, highly reliable and proven approach, continuing to provide a streamlined, highly efficient model that satisfies customer demand while optimizing price performance. The Performance Work Statement (PWS) Sections 2.0, 3.0, and 5.0 describe the NEACC mission.

PWS Section 4.0 describes the tasks that can be ordered via Indefinite Delivery Indefinite Quantity (IDIQ) Task Orders to optionally incorporate other NASA Center-specific applications with the goal of establishing a more efficient operating model. These application maintenance and enhancement services are to be accomplished using the PWS 5.0, Delivery Functions.

PWS Section 5.0 also describes a set of Delivery Functions that represent skills, processes, and supporting activities that are leveraged to fulfill the requirements specified in this PWS. These Delivery Functions are required to support both the NEACC requirements and IDIQ Task Order work.

ATTACHMENT J-1

The Lines of Business supported by the NEACC include Enterprise applications, Center-specific applications, and Cross Functional Infrastructure Services. The EAST 2 Contractor shall perform all requirements outlined in this PWS for all applications across all Lines of Business as described in Attachment **J-21**, *Inventory of Enterprise and Center Applications*, **J-22**, *NEACC Support Systems*, and **J-17**, *Center Applications Transition Plan* and identified below:

- Enterprise Applications
 - Financial (FIN)
 - Human Capital and Workforce (HCW)
 - Identity, Credential and Access Management (ICAM)
 - Logistics (LOG)/Real Property Management (RPM)
 - Office of Education (OE)
 - Procurement (PROC)
 - Product Lifecycle Management (PLM)
- Center-Specific Applications
 - MSFC Center Applications (MSFC-CA)
- Cross-Functional Infrastructure Services
 - Business Intelligence (BI)
 - Enterprise Service Bus (ESB)/Center for Internal Mobile Applications (CIMA)
 - NEACC Support Systems (NSS)

2 PROGRAM MANAGEMENT

Program Management consists of the key areas defined below that ensure all aspects of the EAST 2 contract are managed efficiently and according to regulatory requirements, and that the Government's specific needs with respect to the EAST 2 effort are continuously met. Program Management functions also establish the basis for a positive and collaborative working relationship between the Government and the Contractor. The Contractor shall provide Program Management as described in the following paragraphs (PWS elements):

2.1 CONTRACT MANAGEMENT

Contract Management, as defined in this PWS, encompasses the functions of contract administration as well as those of customer relationship management. Contract administration is aimed at managing the terms and conditions of the contract. Customer relationship management focuses on establishing a collaborative and mutually beneficial relationship between the Government and the Contractor.

ATTACHMENT J-1

No.	Government Requirements
	<i>Contract Management Requirements</i>
2.1.1	In performance of contract administration functions, the Contractor shall provide a local, single point of contact (POC) with contractual obligation authority for all contract administration functions and activities required in performance of this contract. This POC shall have access to all contract administration data and information related to performance of this contract.

2.2 FINANCIAL MANAGEMENT

Financial Management consists of all business and financial functions required to meet the Government’s reporting requirements.

No.	Government Requirements
	<i>Financial Management Requirements</i>
2.2.1	The Contractor shall plan, track, accumulate, and report contract costs and provide other financial support required to meet the budgeting, cost reporting, billing, and disclosure requirements of this contract.
2.2.2	The Contractor shall prepare and submit <i>Cost Reports</i> in accordance with DRD MA-008.
2.2.3	The Contractor shall prepare and submit the <i>Financial Management Report (533M)</i> in accordance with DRD MA-007.
2.2.4	The Contractor shall uniquely identify each Capital Asset acquired by its unique Work Breakdown Structure (WBS) on the NASA Form (NF) 533M submittal in accordance with NASA Policy Directive (NPD) 9250.1A, <i>Capital Asset Identification and Treatment</i> dated October 8, 2010 or any superseding NASA requirements.
2.2.5	The Contractor shall provide input data to the NASA Planning, Programming, Budgeting, Execution (PPBE) process. This data shall incorporate annual requirements projections in the form of Spend plans that match the PPBE horizon of the next Execution Year plus 5 years as Budget Year (BY), BY+1, BY+2, BY+3 and BY+4.

ATTACHMENT J-1

2.3 PROCUREMENT MANAGEMENT

Procurement Management consists of the acquisition activities required to perform the services and functions specified in the PWS and to accomplish the EAST 2 mission.

No.	Government Requirements
	<i>Procurement Management Requirements</i>
2.3.1	The Contractor shall be responsible for the acquisition of resources to accomplish the EAST 2 mission, which shall be deliverable under this contract with title vested in the Government. These resources shall include, but are not limited to: software, services, maintenance and licensing, excluding equipment, goods, and services provided by agency-wide IT infrastructure, Enterprise and Center-specific applications, and services contracts.
2.3.2	The Contractor shall provide software support agreements as identified in Attachment J-5 , <i>Cost Schedules</i> . The contractor shall coordinate with NASA’s Enterprise License Management Team (ELMT) prior to procuring any software license or software maintenance. This coordination shall be conducted in accordance with NFS 1807.70 <i>Enterprise License Management Team (ELMT) Program</i> , where applicable, prior to purchasing license and maintenance. Corporate licensing agreements may be utilized for the pricing of any software identified in Attachment J-5 , <i>Cost Schedules</i> .
2.3.3	The Contractor shall track and make available to the Government the status of all individual procurements from purchase request through final purchase order, delivery, and acceptance.
2.3.4	The Contractor shall provide all supplies, materials, and services (not otherwise furnished by the Government) required for performing the services and functions specified in the PWS to accomplish the EAST 2 mission.
2.3.5	The Contractor shall implement and maintain procurement controls including Contractor policies and procedures governing standards of conduct, procurement processes and practices, and prevention of waste, fraud, and mismanagement.
2.3.6	The Contractor shall conduct a weekly contract activity telecon and provide the Government an activity’s log to status all contract administration activities. At a minimum, this telecon shall include: the EAST 2 Program Manager, Business Manager, Contract Representative, Subcontract Representative, Contracting Officer, and Contracting Officer’s Representative.
2.3.7	The Contractor, in coordination with the Contracting Officer’s Representative (COR), shall acquire all required software license and software maintenance.
2.3.8	The Contractor shall obtain Government approval for IT purchases and shall follow NPD 2800.1 and NPR 2800.2.

ATTACHMENT J-1

No.	Government Requirements
	<i>Procurement Management Requirements</i>
2.3.9	<p>The Contractor shall:</p> <ol style="list-style-type: none"> 1. Prepare and submit DRD LS-001, <i>Government Property Management Plan</i>, for all Government property for which the Contractor has been furnished or has acquired. 2. Perform user responsibilities for the Installation-Accountable Government Property (IAGP) assigned to this contract. Maintain accountability for the record keeping, physical inventory, financial control and reporting of Government property that does not meet NASA equipment management control criteria. 3. Maintain responsibility for reimbursable shipment of property as required to support service delivery

2.4 PROGRAM SUPPORT

Program Support encompasses activities associated with external and internal NEACC reporting and other program requirements.

No.	Government Requirements
	<i>Program Support Requirements</i>
2.4.1	The Contractor shall prepare and conduct monthly EAST 2 management reviews in accordance with DRD MA-003, <i>Monthly Progress Report</i> .
2.4.2	The Contractor shall track official communications with the Contracting Officer’s Technical Representative (COR) such as requests for information, and transmittals, and provide status concerning all such communications.
2.4.3	The Contractor shall prepare and deliver Contractor Employee Clearance Documents in accordance with DRD MA-002, <i>Contractor Employee Clearance Document</i> .
2.4.4	The Contractor shall prepare and submit an Organizational Conflict of Interest (OCI) Mitigation Plan in accordance with DRD MA-005, <i>Organizational Conflict of Interest Mitigation Plan</i> .
2.4.5	In order to ensure a smooth transition to the follow-on contract to the EAST 2 contract, the Contractor shall develop and deliver a Reprocurement Data Package. The Contractor shall provide the initial reprocurement package within 30 days from the beginning of the period of performance of the last option or award term option exercised. Updates to the reprocurement package will be as required by the Contracting Officer and the Contractor shall provide the final submission at the end of the Contract’s period of performance of the last option or award term exercised. The

ATTACHMENT J-1

No.	Government Requirements
	<i>Program Support Requirements</i>
	reprocurement package shall be delivered in accordance with DRD MA-001, <i>Reprocurement Data Package</i> .

2.5 SECURITY MANAGEMENT

The goal of Information Security Management (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.

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

No.	Government Requirements
	<i>Security Management Requirements</i>
2.5.1	<p>Create and Maintain Information Security Management (ISM) Process</p> <p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Complying with the Government’s ISM policies and procedures. Examples include Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST). See Section 5.5.2, Common Information Technology Security Requirements, in this PWS. 2. Performing continuous analysis of industry best practices or trends and informing the Government of changes that could impact or improve the Government’s ISM process.
2.5.2	<p>Communicate, Implement and Enforce Information Security Management (ISM) Procedures</p> <p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Implementing Government ISM policies (e.g., FISMA) for all Contractor services provided. 2. Supporting the Government’s ISM policy enforcement efforts and providing details of Information security practices to the Government.
2.5.3	<p>The Contractor shall identify an IT Security point of contact (POC) for supporting IT security requirements for the EAST 2 contract. The Contractor shall demonstrate compliance with IT information system security requirements by documenting a system security plan (DRD CF-002, <i>Information Technology (IT) Applications Security Plan (ASP)</i>). The Contractor shall meet 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 Government official, determined in accordance with NPR 2810.1, will serve as</p>

ATTACHMENT J-1

No.	Government Requirements
	<i>Security Management Requirements</i>
	<p>the authorizing official for all such information systems.</p> <ol style="list-style-type: none"> 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 Government data, the Government will determine the system’s FIPS 199 security categorization. For any other information systems provided under this contract or used in performing this contract, the Government 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 Government’s 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, Office of Inspector General (OIG) Audits, General Accountability Office (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 Government’s authorizing official. <p>The Contractor shall enter all required system security documentation into the NSAAR.</p>

ATTACHMENT J-1

2.6 SAFETY, HEALTH AND ENVIRONMENTAL (SHE) REQUIREMENTS

Safety, Health and Environmental (SHE) Requirements ensure that all applicable regulations are followed and that safety is promoted throughout all activities associated with the EAST 2 mission.

No.	Government Requirements
	<i>Safety, Health, and Environmental (SHE) Requirements</i>
2.6.1	<p>The Contractor shall provide, implement, and maintain a comprehensive Safety, Health and Environmental (SHE) Plan, in accordance with DRD SA-001, <i>On-site Safety, Health, and Environmental (SHE) Plan</i> and NFS 1852.223-70, and establish and implement an industrial safety, occupational health, and environmental program that: (1) prevents employee fatalities; (2) reduces the number of SHE incidents; (3) reduces the severity of employee injuries and illnesses; and (4) protects property, equipment, and the environment through the ongoing planning, implementation, integration, and management control of these programs. The SHE Plan shall address each of the following Agency SHE core program requirements in detail that are applicable to the EAST 2 effort:</p> <ul style="list-style-type: none"> a. Management leadership and employee involvement b. System and worksite analysis c. Hazard prevention and control d. Safety, health, and environmental training e. Environment compliance
2.6.2	<p>The Contractor shall report mishaps and safety statistics to MSFC’s Safety and Mission Assurance Directorate/Office in accordance with DRD SA-002, <i>On-site Mishap and Safety Statistics Reports</i>. The Contractor shall submit these reports directly to the NASA Incident Reporting Information System (IRIS) or shall use the forms listed in section 15.4 of DRD SA-002, <i>On-site Mishap and Safety Statistics Reports</i>, to report mishaps and related information required to produce the safety metrics.</p>

ATTACHMENT J-1

3 APPLICATIONS OPERATIONS

The Contractor shall provide Applications Operations as described in the following PWS elements.

No.	GOVERNMENT Requirements
	<i>Applications Operations Requirements</i>
3.0.1	The Contractor shall perform triage and assessments, to include the assignment of a Complexity Factor, on all incidents, maintenance and proposed enhancement service requests in accordance with DRD MA-006, <i>NEACC Operational Model</i> .
3.0.2	The Contractor shall, at the Government’s direction, reassess any maintenance or enhancement service request that the Government determines has been assigned to an incorrect Complexity Factor category. The Contractor shall adjust the Complexity Factor and estimated hours accordingly if the Government determines the assignment to be incorrect.
3.0.3	The Contractor shall explain the rationale for the assignment of a specific Complexity Factor to a maintenance or enhancement service request.
3.0.4	The Contractor shall ensure that all work performed as part of PWS Section 3.1 is coordinated with work performed in PWS Section 3.2 to prevent conflicts in configurable items, release builds, or other areas of potential overlap.
3.0.5	The Contractor shall track and make visible to the Government any changes in complexity assignments that may occur after an Applications Maintenance Service Request is in process in accordance with DRD MA-006, <i>NEACC Operational Model</i> .
3.0.6	The Contractor shall work collaboratively with the Government on the Demand Management backlog to ensure that the planned work is completed in accordance with DRD MA-006, <i>NEACC Operational Model</i> . The Contractor shall notify the Government whenever there is available capacity, so that the Government can assign additional Application Enhancement Service Requests to be processed.
3.0.7	The Contractor shall track and make visible maintenance or enhancement services requests that are in process (i.e. partial completion status of requests in process) and shall provide methods for demonstrating completed service requests and for determining when available capacity exists to begin new work in accordance with DRD MA-006, <i>NEACC Operational Model</i> .
3.0.8	The Contractor shall track and make visible to the Government any changes in complexity assignments that may occur after an Applications Enhancement Service Request is in process in accordance with DRD MA-006, <i>NEACC Operational Model</i> .
3.0.9	The Contractor shall provide access to the Government all data associated with SR's worked within the system to allow for regular surveillance to validate resource alignment consistency. (This includes but is not limited to tracking work, individual assignment with associated skill set, estimated/actual hours against SRs and rolled up to a higher level project goal where applicable).
3.0.10	The Contractor shall ensure the Government-provided online service request

ATTACHMENT J-1

No.	GOVERNMENT Requirements
	<i>Applications Operations Requirements</i>
	system meets the minimum requirements to effectively support both Enterprise and Center-specific applications at Contract Assumption.
3.0.11	The Contractor shall provide a single standard Application Portfolio Management (APM) framework for both Enterprise and Center applications that enables decision making to minimize risk, maximize value, and reduce cost.
3.0.12	<p>The nominal support requirement for this service is normal MSFC duty hours. Normal MSFC duty hours are defined as a 5 day week, Monday through Friday (excluding holidays), 8 hours per day covering the primary business hours, 6 a.m. to 7 p.m., as well as performing remote monitoring with on-call support at all other times.</p> <p>The Contractor shall also provide support during major events, patching/vulnerability corrective activities, system issues or scheduled customer requirements. The additional support may result in after hours, weekend, or holiday work where activities cannot be conducted during normal hours due to unacceptable impacts or service level agreements.</p>

3.1 APPLICATIONS MAINTENANCE

Applications Maintenance describes the core set of operational tasks and service request types that must be performed to sustain the operational system and support capabilities offered by the NEACC:

Applications Maintenance Service Request Types:

- Discrepancy/Break-Fix—request to investigate and correct an incident associated with previously working functionality, where the resolution does not result in a change to any configurable item.
- Master Data—request for a master data record to be added or updated in an Enterprise System (e.g. adding a vendor record to SAP).
- Job Request—request to initiate batch or manually processed jobs to provide specified data output or business process functionality.
- Change Request/Discrepancy—request to investigate and correct an incident associated with previously working or documented functionality, where the resolution results in one or more changes to a configurable item.
- Change Request/Maintenance—request to investigate a condition associated with an operational capability where the resolution may result in one or more changes to a configurable item.

Operational Support Tasks

- All tasks not related to one of the above service request types that are required to keep systems, applications, and platforms operational; to provide for continuity of business processes; and to support NEACC end-users.

ATTACHMENT J-1

No.	Government Requirements
	<i>Applications Maintenance Requirements</i>
3.1.1	The Contractor shall complete Applications Maintenance service requests in all applications identified in Attachment J-21 , <i>Inventory of Enterprise and Center Applications</i> in accordance with Attachment J-4 , <i>Service Level Standards</i> . Applications Maintenance services shall include, but are not limited to: triage of incoming Service Requests, definition and specification, functional and technical requirements analysis, design and development, configuration management, application updates, deployment planning and execution, testing, user assistance and training, supporting documentation, ongoing maintenance, and other operational support.
3.1.2	The Contractor shall complete Applications Maintenance service requests in accordance with DRD MA-006, <i>NEACC Operational Model</i> .
3.1.3	The Contractor shall perform operational support tasks required to keep systems, applications, and platforms operational; to provide for continuity of business processes; and to support NEACC end-users (such as end-user support, Business Warehouse data loads, system refreshes, Business Continuous Volume (BCV) splits, application availability monitoring, recurring meetings and telecons as identified in Attachment J-20 , <i>NEACC End-User Forums</i>).
3.1.4	The Contractor shall complete Discrepancy Break/Fix requests across all Lines of Business according to the service levels defined in Attachment J-4 , <i>Service Level Standards</i> (such as data issue, documentation, online entry, reports, system performance, training, and workflow).
3.1.5	The Contractor shall complete Master Data requests across all Lines of Business according to the service levels defined in Attachment J-4 , <i>Service Level Standards</i> (such as cost center, fund center, vendor, custodian, purchasing group, and release strategy).
3.1.6	The Contractor shall complete Job Requests across all Lines of Business according to the service levels defined in Attachment J-4 , <i>Service Level Standards</i> (such as execute batch job request, execute scripts to correct data issue, execute reports or jobs to collect and prepare data in support of audit requests, and internal tracking of software patching).
3.1.7	The Contractor shall complete Change Request/Discrepancy requests in accordance with Attachment J-4 , <i>Service Level Standards</i> and in accordance with DRD MA-006, <i>NEACC Operational Model</i> (such as system functions, database administrator, Enterprise Performance Support System (EPSS) documentation corrections, documentation, printer management, software maintenance, security authorization corrections, system performance and workflow).
3.1.8	The Contractor shall prioritize and escalate service requests based on definitions of severity levels as defined in Attachment J-4 , <i>Service Level Standards</i> .

ATTACHMENT J-1

No.	Government Requirements
	<i>Applications Maintenance Requirements</i>
3.1.9	The Contractor shall ensure that resources assigned to Lines of Business or areas requiring special certifications possess and retain the certifications described in Attachment J-11 , <i>NEACC Certification and Training Requirements</i> .
3.1.10	The Contractor shall complete Change Request/Maintenance requests in accordance with Attachment J-4 , <i>Service Level Standards</i> and in accordance with DRD MA-006, <i>NEACC Operational Model</i> (such as Federal Acquisition Regulation (FAR)/NASA FAR Supplement (NFS) updates; functional checkouts supporting activities external to EAST 2; center re-organization; follow-up requests triggered from end user support calls; other customer requested maintenance activities beyond standard operational support tasks.)
3.1.11	The Contractor shall register all developed Web content via the NASA Web Portal, which is used to catalog all public-facing NASA websites. All required policies and procedures currently approved at the Agency level for this environment shall be adhered to include, but are not limited to, Web Portal guidelines.
3.1.12	<p>The Contractor shall use the Government-provided online service request system. The Government-provided online service request system functions shall include:</p> <ul style="list-style-type: none"> • Tier 2 Incident Management • Tier 2 Service Request Management • Capacity Management of resources • Change Management • Problem Management
3.1.13	The Contractor shall place in an “inactive” status any Applications Maintenance service request that is awaiting input or action from a source other than the Contractor. The Contractor shall actively monitor the inactive status queue and promptly recommence work when the required conditions have been met.

ATTACHMENT J-1

3.2 APPLICATIONS ENHANCEMENT

Applications Enhancement describes the set of service request types that may be performed to enhance the operational support and functional capacity offered by the NEACC.

Applications Enhancement Service Requests include the following two types:

- Applications Enhancement Change Request— Government-approved improvements to NEACC systems, applications, or platforms that result in changes to configurable items.
- Investigation Request—Feasibility study and/or technical assessment for an improvement that may result in an Applications Enhancement Change Request.

No.	Government Requirements
	<i>Applications Enhancement Requirements</i>
3.2.1	The Contractor shall complete Applications Enhancement service requests in accordance with Attachment J-4 , <i>Service Level Standards</i> . Applications Enhancement services shall include, but are not limited to: application updates, definition and specification, functional and technical requirements analysis, design and development, configuration management, deployment planning and execution, testing, user assistance and training, and documentation.
3.2.2	The Contractor shall complete Applications Enhancement service requests in accordance with DRD MA-006, <i>NEACC Operational Model</i> .
3.2.3	The Contractor shall participate in collaborative planning sessions with the Government for the purpose of determining a Target Delivery Date for each service request as it is approved for work to commence. The Government has final approval authority for the Target Delivery Date. The Contractor shall maintain the target delivery date in a current state in the Government-provided online service request system so that it is viewable outside the NEACC.
3.2.4	The Contractor shall track the progress of each service request and ensure that all work is completed in time to meet the Target Delivery Date. The Contractor shall notify the Government within 2 business days of discovering that the Target Delivery Date cannot be met and shall collaborate with the Government to determine a new Target Delivery Date or an alternative course of action. The Target Delivery Date cannot be changed without written Government concurrence. If the Government does not concur with the revised date, the Contractor will be held to the original agreed upon date. The Government has final approval authority for the Target Delivery Date.
3.2.5	The Contractor shall place in an “inactive” status any Applications Enhancement

ATTACHMENT J-1

No.	Government Requirements
	<i>Applications Enhancement Requirements</i>
	service request that is awaiting input or action from a source other than the Contractor. The Contractor shall actively monitor the inactive status queue and promptly recommence work when the required conditions have been met.
3.2.6	In the event that the Government does not accept a service request as completed by the Contractor, the Contractor shall reschedule and complete the service request in accordance with Attachment J-4 , <i>Service Level Standards</i> .
3.2.7	The Contractor shall perform all Applications Enhancement service requests in the most timely manner possible while adhering to the processes defined in DRD QE-001, <i>Software Engineering Quality Plan</i> . These methods shall include iterative processes that enable frequent feedback from functional owners to validate requirements, thorough and iterative testing practices, and reliable coding standards.
3.2.8	The Contractor shall utilize the Government-provided online service request system, as described in PWS 3.1.12, for all work performed under PWS Section 3.2

4 IDIQ OPTIONAL SUPPORT FOR NASA CENTER-SPECIFIC APPLICATIONS

Indefinite Delivery Indefinite Quantity (IDIQ) Task Orders will be used to optionally incorporate other NASA Center-specific applications with the goal of establishing a more efficient operating model. For each Center listed in this PWS section and associated Center facilities, the Contractor shall provide application maintenance and enhancement services using the same Delivery Functions described in PWS Section 5.0. Reserved paragraphs are placeholders for potential future work, and will be added by formal contract modification, if required.

Over time, NASA may decide to migrate these applications to Enterprise services. However, for those applications that remain local, the Contractor shall adhere to local Center CIO governance processes for activities that involve design modification/enhancement of these local services.

The Contractor shall prepare a quote for a Government-requested Task Order, in accordance with NFS 1852.216-80 *Task Ordering Procedure* in Clause **L.12** and *Supplemental Task Ordering Procedures for EAST 2* in Clause **H.20**. The Contractor shall price all Task Orders using the pre-established labor rates in Attachment **J-5A**, *IDIQ Labor Rate Schedule*. The Contractor shall also adhere to NASA Procedural Requirement (NPR) 7120.7, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements*.

ATTACHMENT J-1

No.	Government Requirements
	<i>IDIQ Center-Specific Applications Task Orders Requirements</i>
4.1	AMES RESEARCH CENTER (ARC) (RESERVED)
4.2	ARMSTRONG FLIGHT RESEARCH CENTER (AFRC) (RESERVED)
4.3	GLENN RESEARCH CENTER (GRC) (RESERVED)
4.4	GODDARD SPACE FLIGHT CENTER (GSFC) (RESERVED)
4.5	HEADQUARTERS (HQ) (RESERVED)
4.6	JOHNSON SPACE CENTER (JSC) (RESERVED)
4.7	KENNEDY SPACE CENTER (KSC) (RESERVED)
4.8	LANGLEY RESEARCH CENTER (LaRC) (RESERVED)
4.9	NASA SHARED SERVICES CENTER (NSSC) (RESERVED)
4.10	STENNIS SPACE CENTER (SSC) (RESERVED)

ATTACHMENT J-1

5 DELIVERY FUNCTIONS

Delivery Functions represent skills, processes, and supporting activities that are required to perform the daily function of the NEACC, and that ensure the NEACC is operating at the required performance and quality levels. These same Delivery Functions also apply to the delivery of IDIQ Optional Support for NASA Center-specific Applications Task Orders. The Contractor shall perform all Delivery Functions as identified in PWS Section 5.0 as required to execute activities in PWS Sections 3.0 and 4.0. The Contractor shall provide Delivery Functions as described in the following PWS elements:

5.1 OPERATIONS MANAGEMENT

No.	Government Requirements
	Operations Management Requirements
5.1.0.1	<p>Capacity Management Requirements <i>Capacity Management as defined in this PWS refers to the requirement to track the availability of all resources within the NEACC and to forecast and plan Applications Maintenance Service Requests and Applications Enhancement service request completions activities. This includes reporting of the completion of hours across PWS Section 3.0.</i></p>
5.1.0.2	<p>The Contractor shall implement Capacity Management according to DRD MA-006, <i>NEACC Operational Model</i>, which facilitates the effective operation of the NEACC as described under PWS Section 3.0.</p>
5.1.0.3	<p>The Contractor shall coordinate with the Government on an on-going basis to accurately project the capacity available for upcoming releases.</p>
5.1.1	<p>Service Level Management Requirements <i>The goal of Service Level Management (SLM) is to ensure that all contract Service Level Standards are met and that Contractor performance against Service Level Standards is continuously tracked and monitored.</i></p>
5.1.1.1	<p>The Contractor shall collect and report on all Service Level Standards and performance metrics in accordance with DRD MA-004, <i>Service Level Metrics Report</i>.</p>
5.1.1.2	<p>The Contractor shall review all service requests to validate that Severity Levels have been assigned in accordance with Attachment J-4, <i>Service Level Standards</i>, and to coordinate resolution activities based on the request’s Severity Level.</p>

ATTACHMENT J-1

No.	Government Requirements
	Operations Management Requirements
5.1.1.3	The Contractor shall perform service level communications with the Enterprise Service Desk (ESD) and other Center-specific service desks in coordination with NEACC management.
5.1.2	<i>Release Management Requirements</i> <i>The Release Management strategy sets forth the process for planning, packaging, staging, and deploying all software updates to meet incoming customer demand while managing the risks associated with change.</i>
5.1.2.1	The Contractor’s Release Management process shall adhere to the parameters of the EAST Release and Deployment Management Plan (RDM). The RDM is available on the EAST 2 website at https://www.nssc.nasa.gov/east2 .
5.1.2.2	The Contractor’s Release Management process shall continue the use of all appropriate environments as the Promote-to-Production landscape. The Contractor shall present for approval any changes to these environments to the Government. Only the Government has the authority to approve these changes, and such approval shall be in writing. The Contractor shall, at a minimum, establish and maintain a Promote-to-Production landscape for each application as defined in Attachment J-21 , <i>Inventory of Enterprise and Center Applications</i> .
5.1.2.3	The Contractor shall plan the implementation of releases or other maintenance activity, to include the cutover plan and timing of the deployment of each release or maintenance activity into Production.
5.1.2.4	The Contractor shall execute all steps required to stage, confirm, and deploy the Release in Production environments.
5.1.2.5	The Contractor shall work with the Government to support the NEACC Cross-Organization Review (CORE) and encourage collaboration across the Lines of Business (LoBs); identify and assist in resolving conflicting resources and priorities across LoBs; review inputs of all functional and technical governance forums. The release content determination shall be based on a cross-organizational view of priorities and Capacity and Demand Management.
5.1.2.6	The Contractor shall maintain an Integrated Release Landscape View, incorporating all platforms and applications for each Line of Business that provides a complete view of the Release across the NEACC landscape.
5.1.2.7	The Contractor shall adhere to the guidelines for software release approval as directed by the appropriate Center's governance, policies, and directives.
5.1.3	<i>Quality Assurance Requirements</i> <i>The Quality Assurance program defines policies and procedures to include all aspects of Test Management, Requirements Management, and Development Standards.</i>

ATTACHMENT J-1

No.	Government Requirements
	Operations Management Requirements
5.1.3.1	The Contractor shall prepare, implement and maintain a Quality Assurance Plan that promotes the highest level of performance, reliability, and usability for all NEACC platforms and applications in accordance with DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.1.3.2	The Contractor shall work with the Government’s functional and technical subject matter experts to define the business and technical requirements associated with all Applications Operations and Implementation work. The Contractor shall document functional specifications of all business and technical requirements, including testing requirements, for all Applications Operations and Implementation work in accordance with DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.1.3.3	The Contractor shall execute and document the results of tests for all Applications Operations and Implementation work in accordance with DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.1.3.4	The Contractor shall provide application access for the Government to perform testing verification and validation prior to Release deployment.
5.1.3.5	The Contractor shall locate, verify, and maintain all existing test scripts and procedures used to execute System Integration and Regression testing.
5.1.3.6	The Contractor shall develop and maintain test scripts.
5.1.3.7	The Contractor shall store automated and manual test scripts and shall execute all tests within the Quality Center Test Management tool. The Contractor shall support recurring external and internal audits that relate to Requirements Management and Test Management.
5.1.3.8	The Contractor shall continually maintain and update the existing library of manual and automated regression tests that address the core features and functions of all production applications within the Quality Center Test Management tool.
5.1.3.9	The Contractor shall utilize a system that clearly documents the linkage between an application requirement and the test script(s) that verify or verifies the correct implementation of this requirement. The Contractor shall support recurring audits that seek to verify these linkages.
5.1.3.10	The Contractor shall utilize the Quality Center Test Management tool to document all defects that are discovered during all test phases. The Contractor shall retain all defect documentation for audit purposes in accordance with DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.1.3.11	The Contractor shall collect metrics in the Quality Center Test Management tool on the root causes of defects found during testing.

ATTACHMENT J-1

No.	Government Requirements
	Operations Management Requirements
5.1.3.12	The Contractor shall grant the Government access to the Quality Center Test Management tool for the purpose of viewing and validating test scripts and test results, to perform testing verification and validation and other test procedures, or to perform any other functions requested by the Government.
5.1.3.13	For Commercial Off-the-Shelf (COTS) procurements, the Contractor shall at a minimum verify that each vendor’s VPAT (Voluntary Product Accessibility Template) is complete and correct, and that it conforms to the Section 508 standards and meets the 508 standards for accessibility. A generic Section 508 statement by vendors is not adequate. A VPAT provides relevant information on how a vendor’s product claims to conform to the Section 508 Accessibility standards, and the Contractor shall verify these claims.
5.1.3.14	At a minimum, the Contractor shall provide a Quality Assurance Verification and Validation for 508 compliance as part of its standard software review process, which shall include written documentation of: test results; any 508 guidelines that have not been met; and a remediation plan and timeline for resolving all unmet guidelines.
5.1.3.15	The Contractor shall implement and audit web environments for web site compliance to Federal laws and Agency and Center policies.
5.1.4	<i>Solution Design Requirements</i> <i>Solution Design consists of the processes and skills required to construct integrated solutions that satisfy business requirements within technical constraints.</i>
5.1.4.1	The Contractor shall provide a Solution Design capability that is demonstrated in tangible deliverables that support or facilitate iterative requirements definition over the life of the process.
5.1.4.2	The Contractor shall provide Solution and Application Architecture services that facilitate the overall design and integration of application component systems that are aligned with the Government’s mission objectives and Enterprise Architecture.
5.1.4.3	The Contractor shall adhere to Federal requirements when proposing design solutions. Specifically designs must support Homeland Security Presidential Directive (HSPD)-12-Policy for a Common Identification Standard for Federal Employees and Contractors, and M11-11 <i>Continued Implementation of Homeland Security Presidential Directive HSPD-12.</i>
5.1.5	<i>Configuration Management Requirements</i> <i>Configuration Management consists of a set of processes and tools for identifying, controlling, maintaining, and verifying the versions of all configurable platform, system, and application components.</i>

ATTACHMENT J-1

No.	Government Requirements
	Operations Management Requirements
5.1.5.1	The Contractor shall use the JIRA system to request changes to configuration of NEACC platforms and systems managed by Marshall Information Technology Services (MITS).
5.1.5.2	The Contractor shall use the Government-provided tool to maintain an inventory of NEACC-managed applications. The Contractor shall ensure that all information in this tool is current. The Contractor shall maintain an inventory of custom developed objects for all NEACC-managed applications and ensure the information is current.
5.1.5.3	The Contractor shall maintain and operate a Document Management System that contains controlled versions of all NEACC operational documents.
5.1.6	<i>Business Readiness Requirements</i> <i>Business Readiness consists of the processes and skills required to create and maintain end user documentation and communication that satisfies business requirements and adheres to the Government’s “Business Readiness Approach.”</i>
5.1.6.1	The Contractor shall create or update end user procedures, job aids, and/or training materials as needed to help mitigate the changes introduced to applications and/or services provided by the NEACC, in a standard format; the execution of this work may be entirely the responsibility of Business Readiness (BR) experts or may be done jointly with BPS, Application Functional Support or Information Assurance based on need and expertise.
5.1.6.2	The Contractor shall ensure the business readiness impacts for each service request have been described in accordance with the NEACC Business Readiness Approach Document. The NEACC Business Readiness Approach document is available on the EAST 2 website at https://www.nssc.nasa.gov/east2 .
5.1.6.3	The Contractor shall perform an analysis of the business readiness impacts of each monthly and semi-annual release utilizing the tools specified in the NEACC Business Readiness Approach document.
5.1.6.4	The Contractor shall produce a consolidated view of all the business readiness impacts of the monthly and semi-annual releases for review with the NASA business community, and shall post that information (upon written Government approval) to the bReady portal or its successor.
5.1.6.5	The Contractor shall administer all NEACC content for the NASA training system.

ATTACHMENT J-1

No.	Government Requirements
	Operations Management Requirements
5.1.6.6	The Contractor shall utilize the current NEACC tool for maintaining end user documentation, and shall ensure that the library of end user documentation is maintained and kept up-to-date by searching for and updating all related items with each change as relevant, with particular attention to cross-functional impacts.
5.1.6.7	The Contractor shall support end user training for NEACC applications as requested by the business process owner.

5.2 APPLICATION FUNCTIONAL SUPPORT

PWS Section	Government Requirements
	<i>Application Functional Support Requirements</i>
5.2.1	The Contractor shall provide the functional support knowledge and subject matter expertise required to maintain and support the applications and platforms listed in Attachment J-21 , <i>Inventory of Enterprise and Center Applications</i> and shall update this knowledge as new applications are developed or added to Attachment J-21 , <i>Inventory of Enterprise and Center Applications</i> . Functional support knowledge and subject matter expertise shall include knowledge of application functional configuration; functional integration of applications across Lines of Business (LOB); the skills and abilities required to analyze and trouble shoot problems and inconsistencies within each application; and support digital content creation.
5.2.2	The Contractor shall identify, recommend, and implement, an Incident Management process to prioritize and escalate Application Maintenance and Enhancement tasks as required to continually achieve Expected Service Levels, in accordance with Attachment J-4 , <i>Service Level Standards</i> . The Contractor shall work with the Government to approve the Incident Management process and incorporate into the DRD MA-006, <i>NEACC Operational Model</i> . Approval rests with the Government and shall be in writing.
5.2.3	The Contractor shall execute all test scenarios identified by Operations Management as necessary to support all planned releases.
5.2.4	The Contractor shall coordinate work across all Delivery Functions to ensure that each incident is resolved according to the Incident Management process.
5.2.5	The Contractor shall provide knowledgeable functional support resources to manage the interaction with third party vendors for acquisition, roadmap, and problem resolution.

ATTACHMENT J-1

5.3 APPLICATION DEVELOPMENT

PWS Sections	Government Requirements
	<i>Application Development Requirements</i>
5.3.1	The Contractor shall provide all required skill sets and perform all application development activities required to meet Application Operations and Implementation requirements across all Lines of Business (LOBs) and applications as specified in PWS Sections 3.0 and 4.0.
5.3.2	The Contractor shall utilize Agile software development practices that include an interactive development process which ensures Government and stakeholder involvement. This process shall be applied consistently across all LOBs. The Contractor shall stay apprised of improvements in Software Engineering practices in accordance with DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.3.3	The Contractor shall use consistent Enterprise and Center Coding Standards and Naming Conventions that adhere to DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.3.4	The Contractor shall support all audit activity associated with verifying adherence to Coding Standards and shall promptly respond to and correct any audit findings associated with noncompliance.
5.3.5	The Contractor shall prepare, implement and maintain effective standards for documenting application development designs, individual code components, and associated verification tests in accordance with DRD QE-001, <i>Software Engineering Quality Plan</i> .
5.3.6	Prior to releasing any software into a NEACC Production environment, the Contractor shall ensure that all software developed, enhanced, or modified by the NEACC is accessible to individuals with one or more impairments, as defined in Section 508 of the Rehabilitation Act.

ATTACHMENT J-1

5.4 APPLICATION TECHNICAL OPERATIONS & MAINTENANCE (ATOM)

No.	Government Requirements
	<i>Application Technical Operations & Maintenance Requirements</i>
5.4.1	<p>The Contractor shall design, acquire, build and operate the application technology environment to support the application set for each Line of Business (LOB) and all activities associated with PWS Section 3.0 and 4.0.</p> <ul style="list-style-type: none"> • “Design” shall include creating system and process designs and specifications based on business and technical requirements. • “Acquire” shall include evaluating solution candidates and either procuring systems or establishing service relationships with external providers. • “Build” shall include the establishment of a service capability through installation and configuration of application solutions and end-to-end integration of services provisioned by external providers. • “Operate” shall include monitoring and incident management to ensure availability of all internally-provisioned and externally-provisioned elements of application solutions as well as maintenance activities. <p>This environment shall include the logical and physical software configuration, operational processes, database and other software services.</p>
5.4.2	<p>The Contractor shall apply critical software updates and patches to all NEACC-managed software components for each application. Critical software updates include security updates, updates required to maintain vendor support, and updates required for operational stability.</p>
5.4.3	<p>The Contractor shall ensure that all information system components are up-to-date with all applicable patches which may impact the security of information systems, and shall work with the Government to prioritize non-critical security or bug fix patches.</p>
5.4.4	<p>The Contractor shall provide all required skill sets and shall perform all activities in support of NEACC Application Technical Operations & Maintenance.</p>
5.4.5	<p>The Contractor shall utilize network, computing, storage, business continuity services and end-user services from NASA Integrated Communication Services (NICS), Marshall Information Technology Services (MITS) and Agency Consolidated End-user Services (ACES).</p>
5.4.6	<p>The Contractor shall develop and provide rough order of magnitude (ROM)</p>

ATTACHMENT J-1

No.	Government Requirements
	<i>Application Technical Operations & Maintenance Requirements</i>
	estimates for technology investments.
5.4.7	The Contractor shall develop and provide acquisition options and recommendations for technology investments.
5.4.8	The Contractor shall manage the transition of all new application and infrastructure components into an operational state.
5.4.9	The Contractor shall coordinate and manage all code transports into the Production Systems and throughout non-Production landscapes.
5.4.10	The Contractor shall monitor and manage the execution of interfaces throughout the entire NEACC landscape (includes both production and non-production application instances).
5.4.11	The Contractor shall monitor and manage the execution of all scheduled jobs throughout the entire NEACC landscape (includes both production and non-production application instances).
5.4.12	The Contractor shall maintain a record of all code migrations by application and by release, made throughout all system development landscapes.
5.4.13	The Contractor shall monitor messages for abnormal terminations (includes both production and non-production application instances); notify and record the problem to the respective Government application owners; and provide logs to vendors to support problem resolution.
5.4.14	The Contractor shall perform console operations for applications (includes both production and non-production application instances) including start, responding to messages, monitoring the messages, and stoppage.
5.4.15	The Contractor shall plan and execute comprehensive procedures in support of all planned and unplanned application outages including coordination of interface shut-down, interface start-up, and coordination of batch job scheduling (includes both production and non-production application instances).
5.4.16	The Contractor shall assess and optimize application performance. This includes the establishment and maintenance of a load modeling capability across all LOBs.
5.4.17	The Contractor shall schedule, monitor, and test data backups across the NEACC LOBs.
5.4.18	The Contractor shall provide application administration on infrastructure hardware resources to include adherence to the OCIO guidelines for data structures, development tools, and approved platforms.
5.4.19	The Contractor shall provide engineering services for each LOB to facilitate requirements gathering, landscape management to include maintaining landscape

ATTACHMENT J-1

No.	Government Requirements
	<i>Application Technical Operations & Maintenance Requirements</i>
	drawing, coordinating with hosting organization for new builds, act as a liaison between the NEACC and MITS as needed.
5.4.20	The Contractor shall provide database administration (DBA) for Oracle, MySQL and Microsoft SQL Server to support NEACC applications. These responsibilities include the duties around performance, integrity and security of a database as well as planning, development, and troubleshooting.
5.4.21	<p>The Contractor shall ensure the database approach incorporates the following principles:</p> <ul style="list-style-type: none"> • data remains consistent across the database; • data is clearly defined; • users access data concurrently, in a form that suits their needs; • there is provision for data security and recovery control (all data is retrievable in an emergency).

5.5 INFORMATION ASSURANCE

In order to appropriately secure NASA systems and information, the following IT security requirements apply to the Contractor. 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://www.nasa.gov/offices/ocio/itsecurity/index.html>

No.	Government Requirements
	<i>Information Assurance</i>
5.5.1	<p><i>Information Assurance Requirements</i></p> <p><i>Information Assurance</i> comprises all activities related to ensuring the security of all NEACC platforms and applications, including User Account Management, assignment of application authorizations and roles, business resiliency and disaster recovery planning and operations, and management of the overall Security Lifecycle.</p>
5.5.1.1	The Contractor shall provide Account Management functions for all NEACC applications identified in Attachment J-21 , <i>Inventory of Enterprise and Center Applications</i> , and J-22 , <i>NEACC Support Systems</i> .

ATTACHMENT J-1

No.	Government Requirements
	<i>Information Assurance</i>
5.5.1.2	The Contractor shall provide authorization design, implementation, and operations for all NEACC applications identified in Attachment <u>J-21</u> , <i>Inventory of Enterprise and Center Applications</i> , and <u>J-22</u> , <i>NEACC Support Systems</i> .
5.5.1.3	The Contractor shall provide support for the reporting of Access Management metrics.
5.5.1.4	The Contractor shall provide a business resiliency capability that includes disaster recovery, contingency planning, business continuity, cyber incident response planning, and linkage with like plans throughout the host center, functional Lines of Business (LOBs) and Agency as described in DRD CF-003, <i>Information Technology Service Continuity Management (ITSCM) Plan</i> .
5.5.1.5	The Contractor shall provide security planning in accordance with local, agency and federal guidance.
5.5.1.6	<p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Conducting security reviews and regular audits of information and technology assets under Contractor's control in accordance with the Government's ISM policy. 2. Participating in periodic Government security audits as requested by the Government and coordinating audit activities of Third Parties as required or requested by the Government. 3. Conducting and supporting security penetration testing as required or when requested by the Government in accordance with the Government's ISM policy.
5.5.1.7	The Contractor shall incorporate new projects/programs into the existing security program.
5.5.1.8	The Contractor shall manage routine assessments of security to include privacy assessments, vulnerability assessments, social engineering assessments, segregation of duties assessments, security plan assessments, business resiliency tabletops, business resiliency exercises, and routine reviews of lifecycle improvements to ensure system confidentiality, integrity and availability.
5.5.1.9	The Contractor shall maintain the capability to restore data as of the end of the previous business day for all NEACC production instances utilizing the Government-provided backup services.
5.5.1.10	The Contractor shall provide security awareness training to the NEACC civil servants and contractors.

ATTACHMENT J-1

No.	Government Requirements
	<i>Information Assurance</i>
5.5.1.11	The Contractor shall provide firewall rule analysis and documentation of all rules for systems hosting NEACC applications.
5.5.1.12	The Contractor shall provide process and procedure management for NEACC applications.
5.5.1.13	The Contractor shall provide 24x7 On-Call support for security-related incidents.
5.5.1.14	The Contractor shall provide support for log management and compliance analysis.
5.5.1.15	The Contractor shall coordinate with the Center Security Administrators who manage and support Center access to the Core Financial environment managed by the NEACC.
5.5.1.16	<p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Providing information to the Government to support information asset identification and documentation in accordance with the Government's ISM policy. 2. Providing information to the Government to support information asset review activities regarding completeness, accuracy, and vulnerability. 3. Providing information to the Government to support classification of information assets in accordance with the Government's ISM policy.
5.5.1.17	<p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Monitoring and reporting security breaches and security incidents in accordance with the Government's ISM procedures. 2. Providing information to the Government to support investigation of any security breach and/or security Incident. 3. Providing information to the Government to support resolution of any security breach and/or security Incident.
5.5.1.18	<p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Participating in review and analysis of security breaches and security incidents and creation of security breach and security Incident report. 2. Providing Business Impact Assessment (BIA) on all applications, addressing impact to other applications and/or user community in the event of a short-term or long-term outage.
5.5.1.19	<p>The Contractor shall be responsible for:</p> <ol style="list-style-type: none"> 1. Providing information to the Government to support the assessment of

ATTACHMENT J-1

No.	Government Requirements
	<i>Information Assurance</i>
	<p>security risks.</p> <p>2. Participating in development and maintenance of security improvement plans in accordance with the Government’s ISM policy.</p>
5.5.1.20	The Contractor shall provide analysis against all NEACC end users service to identify all dependencies necessary to provision the service (e.g. PIV card issuance).
5.5.1.21	The Contractor shall adhere to Center incident response processes in addressing perceived IT security incidents/threats and adhere to local Center IT security Continuous Diagnostic and Monitoring (CDM) processes (e.g. Scans, System Security Plan).
5.5.1.22	The Contractor shall provide regular Information Assurance participation in LOB activities including sprint planning sessions, implementation efforts for strategic initiatives, and coordination of security activities.
5.5.1.23	In support of all Center organizations, the contractor shall define and implement the set of processes and activities necessary to integrate applications requiring account management into the NASA Account Management System (NAMS).
5.5.2	<p><i>Common IT Security Requirements</i></p> <p>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), <i>Guide for the Security Authorization of Federal Information Systems</i> 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.)</p>
5.5.2.1	The Contractor shall document its approach to managing information security in an <i>Information Security Management Plan</i> according to DRD CF-001.
5.5.2.2	<p>The Contractor shall configure and maintain application environment on all information systems provided under this contract in accordance with Federal and NASA security configuration policies and guidance.</p> <ol style="list-style-type: none"> 1. The Contractor shall apply all relevant Federal system and software security configurations according to Government guidance. 2. All information systems shall be patched with all critical patches (as determined by the product vendor or the Government) in accordance with the NASA Organization Defined Values for NIST SP 800-53 Security Controls and subsequent revisions. All other applicable patches shall be prioritized in coordination with the Government. 3. In some rare circumstances, the NASA Senior Agency Information Security Officer (SAISO) 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 SAISO or

ATTACHMENT J-1

No.	Government Requirements
	<i>Information Assurance</i>
	<p>his/her designee.</p> <p>4. System configurations and patching status for all information systems provided under and in support of this contract shall be reported using the Government’s patch reporting environment. Each computer shall run up-to-date Government reporting agent software for automated reporting. For any computers that cannot run the reporting agent software, a Government-approved waiver must be obtained in accordance with NASA policy and procedures.</p>
5.5.2.3	<p>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 under the ACES contract. The NASA enterprise anti-malware solution for servers is provided by the NEACC Computing Services (NCS) on the MITS contract. For any computer that cannot use the anti-malware solution or for which no anti-malware software exists, a Government-approved waiver must be obtained in accordance with NASA policy and procedures.</p> <p>The Contractor shall correct or mitigate detected vulnerabilities in accordance with NASA policy, unless directed otherwise by the Government for specific urgent issues.</p>
5.5.2.4	<p>All information systems provided under this Contract or used in support of this Contract shall be scanned for vulnerabilities in accordance with NASA policy.</p> <p>1. The Contractor shall make available all information systems located within the Government’s network perimeter for network-based vulnerability scanning by the Government. The Government will coordinate scanning activities with the Contractor to the extent possible to ensure that vulnerability scanning creates minimal impact on operations.</p> <p>For all other information systems which process Government data, the Contractor shall report to the Government the results of vulnerability scans and remediation, in accordance with NASA guidance.</p>
5.5.2.5	<p>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.</p> <p>1. The Contractor shall verify that all software developers have been successfully trained in secure programming techniques.</p> <p>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)).</p> <p>For web applications, the Contractor shall ensure that the software shall not</p>

ATTACHMENT J-1

No.	Government Requirements
	<i>Information Assurance</i>
	include any of the flaws described in the current "OWASP Top Ten Most Critical Web Application Vulnerabilities."
5.5.2.6	<p>The Contractor shall follow the Government’s 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 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.</p> <ol style="list-style-type: none"> 1. The Contractor shall make available logs from any information system to the Government’s common logging environment, as requested by the NASA SOC. Electronic raw log data shall be forwarded from the source device to the Government’s 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 Government information, in accordance with NASA incident reporting policy and procedures.
5.5.2.7	The Contractor shall provide a logging environment that centrally captures and retains logs from Enterprise information systems provided under this contract as specified by the Government.
5.5.2.8	The Contractor shall provide to the Government 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.
5.5.2.9	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.
5.5.2.10	<p>Prior to deployment of any IT security services, the Contractor shall obtain approval from the NASA Senior Agency Information Security Officer (SAISO) or designee. Any IT security services provided by the Contractor shall be coordinated and integrated with the NASA SOC.</p> <p>Monitoring the Government networks (Government 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 to by the Contractor and the Government and is</p>

ATTACHMENT J-1

No.	Government Requirements
	<i>Information Assurance</i>
	accordingly documented in the Contractor’s <i>Information Security Management Plan</i> , DRD CF-001.
5.5.2.11	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.
5.5.2.12	The Contractor shall work with the NASA OCIO and the incumbent (EAST) Contractor to transfer responsibility for all IT security requirements for existing information systems that are within the scope of the EAST 2 contract from the incumbent Contractor to the successor Contractor. The Government will provide the EAST 2 Contractor a list of the applicable information systems.
5.5.2.13	The Contractor shall perform security incident management, both proactive and reactive.

5.6 CROSS FUNCTIONAL INTEGRATION

The EAST 2 contract relies on Compute services provided by the NEACC Computing Services (NCS) team, which is managed under the Marshall Information Technology Services (MITS) contract.

Success of EAST 2 is dependent upon the ability of the Contractor to work within, and across, other NASA service contracts to ensure a seamless IT service delivery environment and capability across the Agency.

No.	GOVERNMENT Requirements
	<i>Cross Functional Integration Requirements</i>
5.6.1	<i>General Cross Functional Integration Requirements</i>
5.6.1.1	To better enable this Cross Functional Integration, the Contractor shall, at a minimum, implement Associate Contractor Agreements (ACAs), in accordance with H.10 , <i>Associate Contractor Agreements (AUG 2009)</i> , with other Contractors (e.g., other Agency and Center/Facility Contractors) to ensure continuity of service and provide transparency to the Government’s end-users in accordance with defined Service Level Agreements.
5.6.2	<i>Requirements Related to Agency Consolidated End-user Services (ACES)</i> <i>This section identifies the EAST 2 integration requirements with the ACES Contractor. The ACES contract provides a variety of end-user services, e.g., e-mail and collaborative calendaring; end-to-end computing services and back-</i>

ATTACHMENT J-1

No.	GOVERNMENT Requirements
	<i>Cross Functional Integration Requirements</i>
	<i>office infrastructure support; and IT product catalog services to NASA and NASA Contractors.</i>
5.6.2.1	The Contractor shall coordinate with the ACES Contractor to distribute NEACC-managed desktop software.
5.6.2.2	The Contractor shall coordinate and execute the testing of new client-side application components with the ACES Contractor.
5.6.2.3	The Contractor shall collaborate with the ACES Contractor for operations monitoring and incident management.
5.6.3	<i>Requirements Related to NCS and MITS</i> <i>This section identifies the EAST 2 integration requirements with NCS provided by the MITS contract.</i>
5.6.3.1	The Contractor shall adhere to the processes and procedures specified in the NEACC Computing Services Process document. The NEACC Computing Services Process document is available on the EAST 2 website at https://www.nssc.nasa.gov/east2 .
5.6.3.2	The Contractor shall collaborate with NEACC Computing Services (NCS) on the MITS contract for operations and performance monitoring and incident management.
5.6.4	<i>Requirements Related to NASA Integrated Communications Services (NICS)</i> <i>This section identifies the EAST 2 integration requirements with the NICS Contractor. The NICS contract will consolidate LAN and WAN services for the Agency.</i>
5.6.4.1	The Contractor shall collaborate with the NICS Contractor for operations and performance monitoring and incident management.
5.6.4.2	The Contractor shall collaborate with the NICS Contractor on security perimeter configuration for NEACC applications.
5.6.5	<i>Requirements Related to Web Enterprise Service Technologies (WESTPrime)</i> <i>This section identifies the EAST 2 integration requirements with the WESTPrime Contractor. The WESTPrime contract includes public Web site hosting, Web content management and integration, and support of other Web site services.</i>
5.6.5.1	The Contractor shall collaborate with the WESTPrime Contractor as required, should any applications supported by the EAST 2 contract require hosting by the WESTPrime Contractor.
5.6.6	<i>Requirements Related to Enterprise Service Desk (ESD) and the Enterprise Service Request System (ESRS)</i>

ATTACHMENT J-1

No.	GOVERNMENT Requirements
	<i>Cross Functional Integration Requirements</i>
	<i>This section identifies the EAST 2 integration requirements with the ESD (Enterprise Service Desk) Contractor. The ESD contract provides Tier 0/1 Help Desk support services in response to reported incidents and problems, and also provides an integrated service ordering capability for all services.</i>
5.6.6.1	The Contractor shall coordinate with the contractor(s) responsible for the ESD and for other Agency Service Desk tools as required to support the NEACC.