National Aeronautics and Space Administration

Attachment I-1
Performance Work Statement

For

NASA End-user Services & Technologies (NEST) Contract

Table of Contents

1.0 NASA END-USER SERVICES & TECHNOLOGIES (NEST) CONTRACT

1.1 OVERVIEW

The National Aeronautics and Space Administration (NASA) Office of the Chief Information Officer's (OCIO's) mission is to increase the productivity of scientists, engineers, mission support personnel, administrative users, and all NASA organizations in support of NASA's overall mission by quickly and efficiently delivering reliable, innovative, and secure information technology (IT) services. Within the OCIO there are six program offices: IT Security, Data Center/Computing Services, End User Services, Applications, Communications, and Information Management. The End User Services Program Office (EUSO) oversees the portfolio of services and capabilities associated with the end-user services domain; this includes defining and executing overall strategy, roadmaps, standards, policies, investments, and projects.

The scope of EUSO, through direct programmatic authority, includes the following areas: End-User Compute Device Management, End-User Software Management, Mobile Device Management, Print Device Management, Messaging/Collaboration, Infrastructure Services, Enterprise Service Desk (ESD), Local Service Desks, End-User Standards, and IT Security. NASA's overall cybersecurity programmatic authority is the responsibility of the NASA Senior Agency Information Security Officer (SAISO).

The mission of the EUSO is to be the end-user services provider of choice for all of NASA by delivering agile, transformative, and cost-effective services, which align with NASA's evolving leading-edge technology requirements. The EUSO is responsible for delivering excellent service.

NASA considers this a transformational contract. NASA desires to move from a traditional PC (thick client) to a model that is more flexible in addressing customer requirements. This contract seeks to achieve the goals of supporting the NASA workforce in a device-agnostic, mobile friendly environment with built-in security and cloud-based resources. NASA envisions a secure edge computing model similar to eBanking.

To this end, NASA seeks to develop a strategic partnership to transform the end-user experience by providing the necessary agility to support its diverse workforce and mission. The types of support needed for the End User Services Program could include (but are not limited to) desktop engineering, project management support, transformation and operation support, continual service improvement and communications, and other program support functions.

Within this framework, the task of the NEST 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 NEST contract (hereafter referred to as the "Contract") will develop an outsourcing arrangement with the commercial sector to provide and manage the vast majority of NASA's end-user computing hardware, Agency standard software, mobile IT services, peripherals and accessories, associated end-user services, and supporting infrastructure.

1.2 NEST VISION, GOALS, AND OBJECTIVES

1.2.1 Vision

Consistently deliver excellence and provide trusted, readily-available IT services to promote seamless collaboration with internal and external partners for NASA's workforce.

1.2.2 Goals

Goal 1: Provide more flexibility and continuously enhance the user experience.

Goal 2: Seamlessly and transparently implement IT security management and reduce end user impact while implementing.

Goal 3: Provide users with more effective collaboration internally and with external partners.

Goal 4: Serve as effective and innovative partners with NASA Centers, programs, and projects.

1.2.3 Objectives

Objective 1: Improve collaboration and reduce support demand by increasing the adoption of device-agnostic solutions:

- NASA is invested in a transformation from the current traditional PC (thick client) to a model that is more flexible and does not require any special adaptations.

Objective 2: Utilize cloud services.

- The model provides storage of end-user data and quick accessibility in an environment that is secure, sharable, searchable, resilient, accessible, available on all users' devices, and includes Digital Rights Management (DRM) capability as well as data tagging and analytics capabilities.

Objective 3: Enable a zero-trust model

- Enable the creation of microperimeters of control around NASA sensitive data assets and provide visibility into how to use data across the ecosystem.

Objective 4: Provide centralized end-user device management; low- or zero-touch management.

- Provide efficient desk-side support and utilization of self-help and/or walk-in (storefront) help centers.
- Provide zero-touch and automated configuration of new devices and services.

Objective 5: Minimize number of end-user devices and complexity.

- Simplify access to services so fewer devices and types of devices are needed
- Simplify end-user device offering environment (standardize the end-user device)

Objective 6: Refine user profiles/roles.

- Enable the assignment of hardware and software to end users based on their operational duties and needs.

Objective 7: Move the end-user applications to the edge (O365, mobile device management (MDM)).

- Provide application management via an application store for NASA-approved commercial off-the-shelf (COTS) and in-house-developed applications and software.
- Provide expanded access to state-of-the-art collaborative tools and capabilities including instant messaging, online/web meetings, personal video conferencing, shared workspaces, social media, professional networking, and workgroup support systems that will enhance NASA's ability to conduct business securely.

Objective 8: Transparency

- Provide a user-friendly dashboard to provide EUSO Program Executive (PE) (and others), CRMs, and Center CIOs with information about the quality of service by Center and throughout NASA. The data must be dynamic so the user can drill into metrics.

Objective 9: Partner with NASA to create transformative roadmaps for innovations and integration.

- Develop transformative roadmaps enabling secure smart innovations, infrastructure, and integration across all services including sharpened virtual technologies, cloud services, and secure remote access. These roadmaps will address the uncertainties inherent to changes in technology by addressing development and design through prototyping, testing, and evaluation of costs for implementation of new technologies to place NASA in a healthy IT posture.
- Partner with NASA to set goals for the design, development, implementation, and management of virtual service solutions in order to fully realize transformative and innovative data-centric solutions. Early transformations include virtual desktop infrastructure VDI solutions and improved security that enables a device-agnostic environment.

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 EUSO services. The Government will also retain authority for all demand management, governance, and approval functions associated with the EUSO and the NEST Contract.

1.4 GENERAL DESCRIPTION OF WORK REQUIREMENTS

The Contractor shall provide all resources to acquire, provide, install, test, manage, plan, design, integrate, upgrade, operate, secure, and maintain all NASA-approved hardware and software in support of NASA's End User Computing hardware, Agency standard software suite, mobile IT services, printers and multi-functional devices (MFDs), NASA service catalog of IT services and accessories, Tier 2 and 3 support, priority services (VIP), enhanced support services, and supporting infrastructure for all services as delineated in the NEST Performance Work Statement (PWS). The NEST standard business hours are 6:00 a.m. to 6:00 p.m. local time, Monday through Friday (excluding Federal holidays), for locations identified in section 1.5 Service Locations.

Additionally, with Government approval, the Contractor shall research, propose, recommend, and implement new systems/software, replacement and/or deletion of systems/software or enhancements to existing systems/software in support of NASA's IT transformation objectives based on proven industry best practices and in accordance with NASA's EUSO objectives and programmatic requirements.

1.5 SERVICE LOCATIONS

The NEST services shall be performed at the NASA sites listed in Table 1.5-1. Additional performance sites may be identified throughout NEST Contract execution. Near-site support shall be provided to businesses or Government agencies within a 10-mile radius as defined in Attachment I-24, *Glossary of Terms*.

Table 1.5-1. NASA Service Performance Sites.

* Ames Research Center (ARC)
* Armstrong Flight Research Center (AFRC)
AFRC – NASA Armstrong Building 703 (Palmdale, CA)
* Glenn Research Center (GRC)
GRC – Plumbrook Facility (Sandusky, OH)
GRC – NASA Safety Center (Cleveland, OH)
Goddard Space Flight Center (GSFC)
GSFC – Wallops Flight Facility (WFF) (Wallops Island, VA)
GSFC – White Sands Complex (WSC) (Las Cruces, NM)
GSFC – Independent Verification and Validation Facility (IV&V) (Fairmont, WV)
GSFC – Goddard Institute for Space Studies (GISS) (New York, NY)
GSFC – Columbia Scientific Balloon Facility (CSBF)
Headquarters (HQ)
HQ – JPL NASA Management Office (Pasadena, CA)
HQ – NASA at Long Beach, CA
Johnson Space Center (JSC)
JSC – Neutral Buoyancy Laboratory (NBL)
JSC – White Sands Test Facility (WSTF)
JSC – El Paso Hangar (El Paso, TX)
JSC - El Paso Forward Operating Location (El Paso, TX)
Kennedy Space Center (KSC)
KSC – Vandenberg Air Force Base (VAFB)
Langley Research Center (LaRC)
Marshall Space Flight Center (MSFC)
MSFC – Michoud Assembly Facility (MAF)
MSFC – National Space Science & Technology Center (NSSTC)
MSFC – Communications Service Office (CSO) (Wynn Drive building)
* NASA Shared Services Center (NSSC)
* Stennis Space Center (SSC)
SSC – Infinity Science Center (ISC)

Key: * Designated as Small Centers (Reference I-8, Award Term Option Plan, Table ATO-TP-8.2)

Hereafter, "Center(s)" will refer to NASA Center(s) and associated facilities.

2.0 PROGRAM MANAGEMENT

Program Management consists of key areas defined below that ensure all aspects of this Contract are managed efficiently and effectively and in accordance with sound business practices and regulatory requirements to ensure the Government's programmatic requirements are satisfactorily achieved. The Contractor's Program Management Office, including the Program Manager (PM) and other critical staff positions shall be physically located in Huntsville, AL.

The PM shall have local autonomy, to include management, contractual, and financial authority, to make local programmatic changes and decisions on behalf of the Contractor in conjunction with EUSO. Program Management functions establish the foundation for a collaborative and positive working relationship between the Government and the Contractor.

2.1 PROGRAM SUPPORT

Program Support encompasses all activities associated with all EUSO reporting and other Agency program requirements. The Contractor shall:

a. Prepare and conduct monthly EUSO management reviews in accordance with Attachment I-2, *Data Requirements Description* (DRD) MA-07, *Program Management Report*.
b. Track official communications with the Contracting Officer's Representative (COR) such as requests for information, Task Order Requests, and transmittals, and provide status on all such communications.
c. Prepare and submit an Organizational Conflict of Interest (OCI) Mitigation Plan in accordance with Attachment I-2, DRD MA-09, *Organizational Conflict of Interest Plan*.
d. Establish Associate Contractor Agreements (ACAs) and shall ensure seamless program and operational integrations with multiple provided programs and services with limited impact to all end-user services. Program integration support for the EUSO currently includes all contracts identified in the Model Contract section 6.10, Associate Contractor Agreements, and others that may be identified by the Contracting Officer (CO) during performance of this Contract.
e. In partnership with NASA and other contractors, develop, update and maintain all business rules, Standard Operating Procedures (SOPs), and any other process-related documentation (i.e., Service Transition, Service Operations, Service Delivery, etc.). The frequency of updates shall be annually or within 30 calendar days from any major business rules, SOPs, or such related activities changes. The EUSO will have final approval of these deliverables, and the Contractor shall provide the Government advance notification prior to any deviations from processes outlined in the aforementioned documents. The format will be jointly determined by the Government and Contractor, but the contents of the documents shall align with the Information Technology Infrastructure Library (ITIL) Service Management Framework (Version 3 and any subsequent revisions).
f. Understand changing and emerging conditions and business needs as they relate to user services and service offerings and proactively address any changing technologies.
g. Work with EUSO Communications and other Program stakeholders, including the ESD, to understand how different Center or Mission end users may be impacted differently by the same change or release and how to account for that impact.
h. Continually review and analyze End-user Standards (e.g., 2804 & 2805) and proactively provide comments to the EUSO Program Manager and COR on operational or service impacts, and risk assessments/mitigations of all upcoming standard changes.
i. Detail in Attachment I-19, *Management Plan*, how the Contractor will communicate with the Government, other contractors, customers, and end users, in accordance with Attachment I-2, DRD MA-01, *Management Plan*.

2.1.1 Critical Staffing Positions

The Contractor shall hire and retain the following Critical Staffing Positions, which shall be located on-site at NASA MSFC in Huntsville, AL or designated Centers as listed below:

Staffing Positions	Location
a. Program Manager	Huntsville, AL
b. Deputy Program Manager	Huntsville, AL
c. Center Operations Manager	All Centers

   i. One (1) Center Operations Manager shall be located on-site at each NASA Center, except for SSC, in which the SSC Center Operations Manager will also provide support to the NSSC.

The government shall reserve the right to periodically review and unilaterally update the requirement Critical Staffing Position locations. This may require the contractor to update critical staffing position locations to the original requirement outlined at the time of contract award.

2.2 PROJECT MANAGEMENT

The Contractor shall adhere to NASA Procedural Requirement (NPR) 7120.7, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements* (see Attachment I-2, DRD MA-01, *Management Plan*).

2.3 COMMUNICATION OUTREACH AND END-USER TRAINING

The Contractor shall be responsible for a Communication Outreach and End User Training process that complements the EUSO Communications processes as defined in EUSO SOP-CFS1500, *EUSO Communication Processes*.

2.3.1 Communication Outreach

The Contractor shall:

a. Conduct proactive end-user outreach activities in coordination with and at the discretion of the EUSO Communications Lead, ensuring all communication is aligned with and approved by EUSO.
b. Work closely with EUSO to ensure Contractor-provided products and services are ordered, approved, and communicated to end users in a consistent manner using established processes and Section 508-compliant formats. The Contractor shall coordinate communications with the end users through the Government-established communication POCs.
c. Provide users with information and educate end users on available or upcoming user devices, services and service offerings.
d. Assist end users with obtaining end-user services through the service ordering procedures, using Government-defined tools or understanding the impact of production environment changes and releases.
e. Perform outreach regarding general information to users (e.g., services and descriptions) and changes to the end-user environment (e.g., introduction of new products/services, upgrades, outages, maintenance downtime, and special events).
f. Develop outreach with sufficient lead time to allow for Government review, edits, and final approvals prior to distribution to end users, as outlined in EUSO SOP-CFS1500.
g. Manage and/or develop content for the following outreach/communication tools, which include, but are not limited to, the following products/services (as described in the EUSO SOP-CFS1500):
    - Communication Plans
    - User Newsletter (or contribution to existing)
    - User Web Site (or contribution to existing)

- User Training (e.g., User Guides, Quick Start Guides, FAQs, Face-to-Face (F2F) Training at Centers such as Town Halls, Virtual Training, Instructional Videos)
- Agency-wide communication (to all users)
- Direct, targeted communication (email to segmented impacted users (e.g., all Mac users, all Windows users))
- Develop, manage, and publish Knowledge Articles (KA)/Other Service Desk Readiness to expand end-users' knowledge and understanding of Contractor-provided services and service offerings, including providing educational and instructional information based on trouble call and service desk historical trend data to prevent future incidents and problems. Knowledge Articles shall be submitted through NASA's IT Service Management (ITSM) system.

h. Establish and maintain appropriate distribution lists for targeted communication (e.g., different OS types, Center-specific, contractor and non-contractor-provided systems.)
i. Provide communication support for all testing and deployments to users including pilots, early adopters and general deployment.
j. Integrate with the EUSO Customer Relationship Management (CRM) functional leads and CRM Center representatives as indicated by the EUSO. Each EUSO CRM will identify IT POCs at their Center for the Contractor to partner with, guide, or provide insight into the various technical aspects of the Contract. The Contractor shall provide a corresponding technical contact for each Center for the major technical portions of the Contract.
k. Ensure that end-user documentation includes documentation on the end user's specific system hardware to explain the functions of buttons on their device(s) and how to program the system's programmable function keys.
l. Develop and maintain online end-user documentation on all Contractor-provided services, including commercially available products (e.g., Microsoft Office user guide), where available from the vendor. The documentation will show how to use each function of the provided version of the product or service.
m. Develop and maintain Contractor online documentation for Contractor services, such as a service catalog user's guide. All documentation will be reviewed and approved by EUSO Communications prior to its availability to the end-user community.
n. Work with EUSO Communications and other Program Stakeholders to understand how different Center or Mission end users may be impacted differently by the same change or release, and how to account for that impact via modified documentation.

2.3.2 End-User Training

To ensure NASA end users have the information and resources they need to understand changes and new services introduced to the NASA environment, the Contractor shall:

a. Provide all end users with online familiarization training for all Contractor-managed hardware and software products. The end-user training shall include Quick Tips and clearly delineate all changes and/or new features and/or changes in functionality.
b. Provide end-user familiarization training for NEST-provided/supported hardware and software products and services. The Contractor shall detail its planned end-user training approach in Attachment I-19, *Management Plan*, prepared and submitted in accordance with Attachment I-2, DRD MA-01, *Management Plan.*
c. Offer a range of additional training courses covering the breadth of Contractor-provided/supported products/services and access to tutorial videos.

d. Provide assistance to end users in the use of end-user-configurable services and settings for all provided products and services, as well as guide them in the appropriate use of the provided products and services.
e. Develop, maintain and provide training to NASA users, for all changes to NASA's environment (e.g. virtual, video, user guides).

2.3.3 End-User Documentation

The Contractor shall:

a. Provide end-user documentation which may take several forms, including but not limited to online help, help files, tutorials, PDF documents, and printed manuals.
b. Ensure that end-user documentation includes documentation on the end user's specific system hardware to explain the functions of buttons on their device(s) and how to program the system's programmable function keys.
c. Ensure all end-user documentation is 508 compliant.
d. Develop and maintain online end-user documentation on all Contractor-provided services, including commercially available products (e.g., Microsoft Office user guide), where available from the vendor. The documentation will show how to use each function of the provided version of the product or service.
e. Develop and maintain Contractor online documentation for Contractor services, such as a service catalog user's guide. All documentation will be reviewed and approved by EUSO Communications and ESD prior to its availability to the end-user community.
f. Work with EUSO Communications, ESD, and other Program Stakeholders to understand how different Center or Mission end users may be impacted differently by the same change or release, and how to account for that impact via modified documentation.

2.3.4 Home Use Software

Home Use Software includes software in which license agreements permit a free or discounted price for employee purchase and use on employee owned computers. Examples include Microsoft Home Use Program (HUP). The contractor is not responsible for software ordering, provisioning, or management of employee purchased software.

The Contractor shall:

a. Facilitate NASA and contractor employee utilization of software for home use to the extent that the Government or the Contractor are able to obtain such a right from a software publisher, and Government determination that such software shall be eligible for use on employee-owned computers.
b. Provide knowledge articles including instructions for employee home use software ordering and receipt.

2.4 STRATEGIC PLANNING AND TECHNOLOGY EVALUATION

NASA is committed to the continual improvement of its processes, practices, and products. The Contractor is expected to embrace this commitment and to provide the program vision and leadership required to ensure the proper focus on continual improvement and innovation. This includes innovations in management resulting in process improvements or enhanced customer service, as well as technical innovations resulting in increased quality or reliability of the EUSO operations and services. The Contractor shall:

a. Provide technical information concerning any invention, discovery, improvement, or innovation made by the Contractor in the performance of work under this contract.

b. Derive and document recommendations for the EUSO processes and productivity improvements in areas of this PWS.
c. Due to the evolving nature of the EUSO, evaluate, recommend, and provide operations support necessary to enable NASA success based on technology changes.

2.5 SERVICE LEVEL AGREEMENTS AND PERFORMANCE METRICS

Service Level Agreements (SLAs) are used to objectively measure the Contractor's technical performance, a determining factor which the Award Term Evaluation Board (ATEB) uses in combination with the subjective evaluation criteria for Program Management Performance, to determine Award Term Option decisions (see Attachment I-8, *Award Term Option Plan*). The Contractor shall:

Track, manage, and report SLAs for Attachment I-3, *Service Level Agreements*, 1.1 Service Delivery, 1.3 Incident Management, and 1.5 Service Asset and Configuration Management within NASA's ITSM system.

a. Develop Operating Level Agreements (OLAs) with the Government or Government-managed 3rd parties to ensure the Contractor can reliably make use of existing processes and systems outside of Contractor control which shall work together to meet the SLAs in Attachment I-3, *Service Level Agreements*.
b. Ensure that the Management Plan describes the Contractor's approach to managing SLAs and OLAs between the Contractor and the Government and Government-managed 3rd parties to ensure continuity, compliance, and a positive impact on the end user's experience.
c. Ensure that any proposed SLA exclusions are submitted in writing and evaluated in advance by the Government; SLA exclusion requires written approval from the COR prior to exclusion from the SLA calculation.

2.5.1 Changes to Service Level Agreements (SLAs) and Performance Metrics

The Contractor and Government shall periodically review, no less than annually, and make recommendations with regards to any proposed additions, deletions and updates to the metrics and performance standards in Attachment I-3, Service Level Agreements. The overall goal is to be able to measure and continually improve service delivery and customer satisfaction of all NEST services. Any proposed changes shall be discussed as part of the regularly scheduled Program Management Reviews. All accepted proposed changes to the SLAs, including effective dates and applicability of any changes to the SLAs, is subject to a mutual agreement of the parties. Upon approval, the changes will be incorporated via a bilateral contract modification.

2.6 RISK MANAGEMENT

The Contractor shall:

a. Provide risk analysis and management that includes continual identification and assessment of technical, schedule, cost, security, and organizational risks involved with the delivery, operations, and decommissioning of services and system under this Contract. The Contractor shall prepare and submit a risk management approach in accordance with Attachment I-2, DRD MA-01, *Management Plan*.
b. Identify and characterize IT-related risks, devising mitigation steps and monitoring risks and mitigation activities on an ongoing basis.
c. Perform risk assessments and define risk mitigation processes in accordance with NASA Procedural Requirement (NPR) 7120.7.

d. Perform Cybersecurity Risk Management in accordance with requirements in NASA ITS-HBK 2810.04-01, Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching, and Organizationally Defined Values.
e. Provide support in drafting risk management plans and risks for future EUSO services.
f. Support implementation of the EUSO Risk Management Plan.

2.7 CONTRACT PHASE-IN/IMPLEMENTATION MANAGEMENT

The Contractor shall provide a detailed Contract Phase-In and Implementation approach in its Phase-In Plan, in accordance with Attachment I-2, DRD MA-03, *Phase-In Plan*.

2.8 ENTERPRISE IT SERVICES PROGRAM INTEGRATION

The NEST Contract is part of the NASA OCIO's Enterprise IT Services strategy, which spans across the following services: Network Communications, End-user Services, Enterprise Applications, and NASA's Shared Service Center (NSSC) Next Generation contract (NSSC NexGen). Success of NASA's Enterprise IT Services is dependent upon the ability of Enterprise IT Services Contractors to work within, and across, independent service contracts to ensure a seamless IT service delivery environment and capability across the Agency. To effectively support this OCIO programmatic structure, the Contractor shall:

a. At a minimum, implement ACAs with Enterprise IT Services Contractors and other Contractors (e.g., other Agency and Center Contractors) to ensure continuity of service and provide transparency to the NASA end-users in accordance with defined Service Level Agreements.
b. Ensure consistency with the ITIL framework and NPR 7120.7, NASA IT and Institutional Infrastructure Program and Project Management Requirements by hosting Process Integration Workshops to develop a shared understanding of how the Contractor needs to work with the other Enterprise Service and Integration (ES&I) stakeholders.

2.8.1 NASA Integrated Communications Services (NICS)

The NEST integration requirements with the NICS Contractor includes the following integration support services. The NICS contract consolidates Local Area Network (LAN) and Wide Area Network (WAN) services for the Agency. The Contractor shall obtain telecommunications services from NICS or other contractors; in addition, the Contractor shall:

a. Obtain all WAN services required to support provisioning of NEST services from NICS.
b. Obtain all LAN services required to support NEST from NICS, when NICS is the service provider. For Centers that have a Contractor other than NICS provisioning LAN services, the Contractor shall obtain those services from that Contractor and coordinate such services with NICS.
c. Obtain Internet Protocol (IP) address space and Domain Name System (DNS) services from NICS following NICS-provided processes.
d. Obtain Network Time Protocol services from NICS when NICS is the service provider for these services.
e. Obtain all communications services required to support NEST from NICS when NICS is the service provider for these services.
f. Coordinate with NICS for integrated NEST/communications services when NICS is the service provider for these communications services.

2.8.2 Enterprise Applications Service Technologies 2 (EAST-2)

This section identifies the NEST integration requirements with the EAST-2 contractor. The EAST-2 contract provides support of existing operational applications and systems, as well as improvements and additions to existing capabilities. The Contractor shall:

a. Coordinate with Enterprise Architect (EA) from EAST-2 to obtain the distribution package for EAST-2 managed desktop software.
b. Validate EAST-2 software distribution packages in the NEST environment for successful deployment. If validation is unsuccessful, the Contractor shall notify the EAST-2 Contractor.
c. Deploy EAST-2 software distribution packages to end-user client desktops.
d. Obtain EAST-2 managed end-user accounts using EAST-2 defined processes and procedures.
e. Coordinate with EAST-2 to ensure proper provisioning of two-factor user authentication tokens and certificates prior to distribution.
f. Support outward facing websites and public website hosting services, content management, integration and support for other Web site services (formerly services provided by the WESTPrime contractor).
g. Coordinate with EAST 2 for integrated NEST/application services when EAST 2 is the service provider for these applications services.

2.8.3 NSSC Next Generation (NexGen)

The ESD serves as the single point of entry for all NASA IT customers as well as some Center/Mission Directorate specific services. The Service Provider (SP) staffs the ESD to receive and respond to customer inquiries made via Tier 0, existing telephone (1-877-NSSC123), and email (nasa-esd@mail.nasa.gov). ESD personnel possess knowledge of IT services and are able to use knowledge-based tools to accurately respond to and resolve routine customer inquiries at initial contact. Contacts that cannot be resolved at Tier 1 shall be promptly referred to the appropriate Enterprise IT Services Provider, Center or Mission Directorate personnel for resolution. The ESD continually searches for ways to utilize self-service Tier 0 solutions while maintaining high customer satisfaction. The ESD maintains the confidentiality of proprietary, personal, and sensitive information in accordance with NASA policy and all relevant and current laws and regulations. The ESD service elements include the capability to track customer inquiries from initial inquiry to final resolution. The ESD maintains a history of all requests from customers for assistance, including resolution. The ESD manages and uses NASA's ITSM system that the NEST Contractor will also be using.

ESD Service Elements:

- Incident Management
- Service Request Management
- Service Definition Workflow
- Configuration Management
- Real-time User Surveys
- Knowledge Management
- Communications, Service Outages and Notifications
- Change Management
- Problem Management

- ESD Support for Other Agency IT and non-IT Helpdesks or Services

3.0 CONTRACT MANAGEMENT

The Contractor shall implement an overall management approach and the activities necessary to perform the core functions required under the Contract, in accordance with Attachment I-2, DRD MA-01, *Management Plan*. Contract management encompasses the functions of Contract administration that is aimed at complying with the terms and conditions of the Contract and working to establish a collaborative and mutually beneficial relationship between the Government and the Contractor. The CO at the NASA Shared Service Center (NSSC), Stennis Space Center, and the NEST COR in Huntsville, AL, are the primary Government interfaces to the Contractor for contract management.

3.1 CONTRACT ADMINISTRATION SUPPORT

In performance of contract administration functions, the Contractor shall:

a. Provide a Contract Manager with contractual authority for all contract administration functions and activities required in performance of this Contract.
b. The Contract Manager shall have full access to all contract administration data and information related to the contract management and performance of this Contract and shall work proactively with the CO and COR to ensure overall contract success in support of the EUSO.
c. Provide online access to contract administration information and other required data to the CO and other designated personnel, in accordance with NASA Policy Directive (NPD) 1440.6x NASA Records Management.
d. Provide and maintain a listing of all on-site and off-site Contractor and subcontractor employees working under the Contract and their designated locations in accordance with Attachment I-2, DRD MA-04, *Employee Listing*.
e. Provide and maintain a report of Lost, Damaged, Destroyed, or Stolen contractor property in accordance with Attachment I-2, DRD IT-03, *Lost, Damaged, Destroyed, and Stolen Property Report*.
f. Generate, edit, merge, maintain, and distribute documentation related to the performance of this Contract to include documents, storage media, and records.

3.2 FINANCIAL MANAGEMENT

a. The Contractor shall perform all business and financial functions necessary to fulfill the requirements of the Contract and integrate these functions across all areas of performance.
b. The Contractor shall provide ongoing business analysis and respond to requests and inquiries from the Government relating to budget. In performing these functions, the Contractor shall:
    i. Track and manage requests for invoice or service asset discrepancies identified by the Government and report them on a monthly basis per Attachment I-2, DRD MA-07, *Program Management Report*. The Government expects corrections to identified discrepancies to be made within 5 business days within the NASA ITSM system.
    ii. Present monthly invoices in accordance with the invoicing clauses of the Contract. The monthly invoices shall identify the Center.
    iii. Provide documentation to the EUSO Manager that appropriate tax exemptions have been applied for as related to the applicable Centers and/or facilities.

iv. Provide financial and budget information maintained by the Contractor for use by the Government for budgeting purposes and business case analyses (e.g., Program, Planning, Budget and Execution, and Office of Management and Budget (OMB) Exhibit 300, and the Capital Planning and Investment Control (CPIC) process).

v. Employ an approach that allows invoicing to be standardized for each Center. In addition, this approach shall provide the ability for invoice segregation by Centers carrying appropriate allowances and billing methodology. This approach shall also provide specific details related to the individual orders.

3.3 RECORDS MANAGEMENT

a. The Contractor shall ensure that accurate and complete records (including vital records) of Government business are maintained in accordance with Federal requirements and NPR 1441.1x, *NASA Records Management Program Requirements*, and NRRS 1441.1, *NASA Records Retention Schedules*, and are segregated from company-owned records and from non-record materials. The term "records" is defined in 44 U.S.C. 3301 as:

"all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included."

All data created for Government use are Federal records subject to the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33; the Freedom of Information Act (FOIA), as amended; and the Privacy Act, and must be managed and scheduled for disposition as provided in 36 CFR XII, Subchapter B.

b. The Contractor shall meet the following specific records management requirements:

i. Maintain a records management program and submit a Records Management Program Plan in accordance with Attachment I-2, DRD MA-05, *Records Management Program Plan.*

ii. Provide NASA or authorized representatives with access to all Government records. The Government reserves the right to inspect, audit, and copy record holdings.

iii. Manage legacy Federal records (data created for Government use and delivered to or falling under the legal control of the Government) inherited from previous contracts.

iv. At the completion or termination of the Contract, leave all Government-owned records at the Center for which the data were generated, and deliver or disposition the records as directed by the appropriate Center records manager.

v. Delivery of records shall include sufficient technical documentation of all electronic records to permit Government access and use.

3.4 QUALITY MANAGEMENT

The Contractor shall detail its planned quality controls in Attachment I-19, *Management Plan*, prepared in accordance with Attachment I-2, DRD MA-01, *Management Plan.*

3.5 SAFETY, HEALTH, AND ENVIRONMENTAL

a. The Contractor shall provide, implement, and maintain a comprehensive Safety and Health Plan, in accordance with NASA Federal Acquisition Regulation (FAR) Supplement (NFS) 1852.223-72, *Safety and Health Plan (Short Form)*, in accordance with Attachment I-2, DRD SA-01, *Safety and Health Plan*.
b. The Contractor shall prepare and submit reports used to complete the annual report to NASA Headquarters on affirmative procurement, waste reduction, energy efficient product procurement, and ozone depleting substances, in accordance with Attachment I-2, DRD MA-08 *Electronic Product Environmental Assessment Tool (EPEAT) Purchases Report*.

3.6 PROPERTY MANAGEMENT AND COORDINATION

The Contractor shall prepare and submit Attachment I-2, DRD MA-02, *Property Management Plan*, for all Government property for which the Contractor has been furnished and/or has acquired on behalf of the Government. Property management shall be conducted in accordance with Attachment I-17, *Government Property Management Plan*.

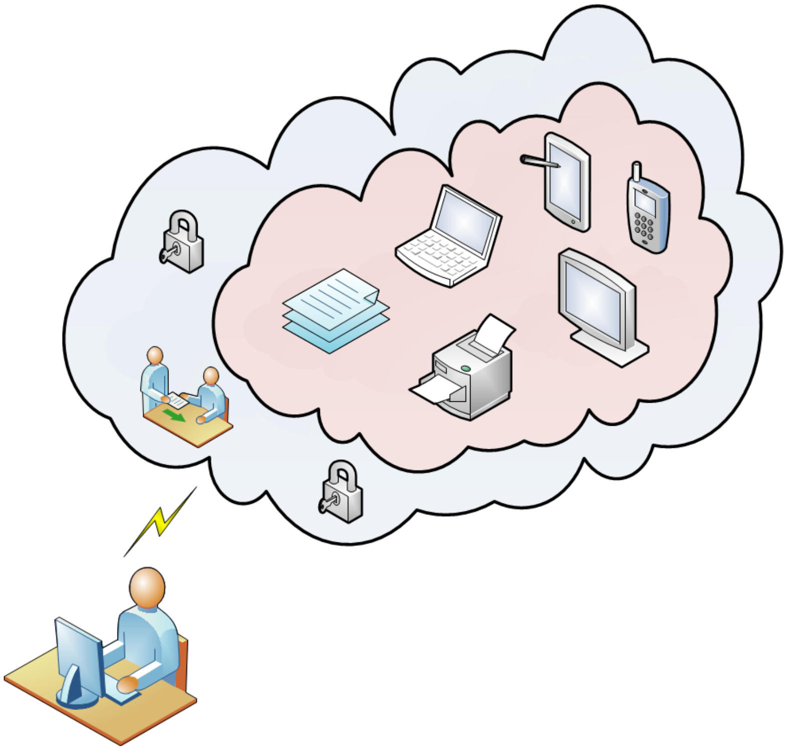
3.7 EMERGENCY PREPAREDNESS AND RESPONSE

a. The Contractor shall provide a Disaster Recovery/Continuity of Operations Plan for each Center in accordance with NASA's policies and procedures (i.e., National Institute of Standards and Technology (NIST) SP 800-53 (Revision 4), *Recommended Security Controls for Federal Information Systems and Organizations*).
b. The Contractor shall comply with Center emergency management plans.
c. The Contractor shall prepare and submit Attachment I-2, DRD IT-05, *Continuity of Operations Plan* (COOP) and ensure that all applicable personnel are trained in emergency management operations in accordance with this plan.

4.0 TRANSFORMATION AND INNOVATION

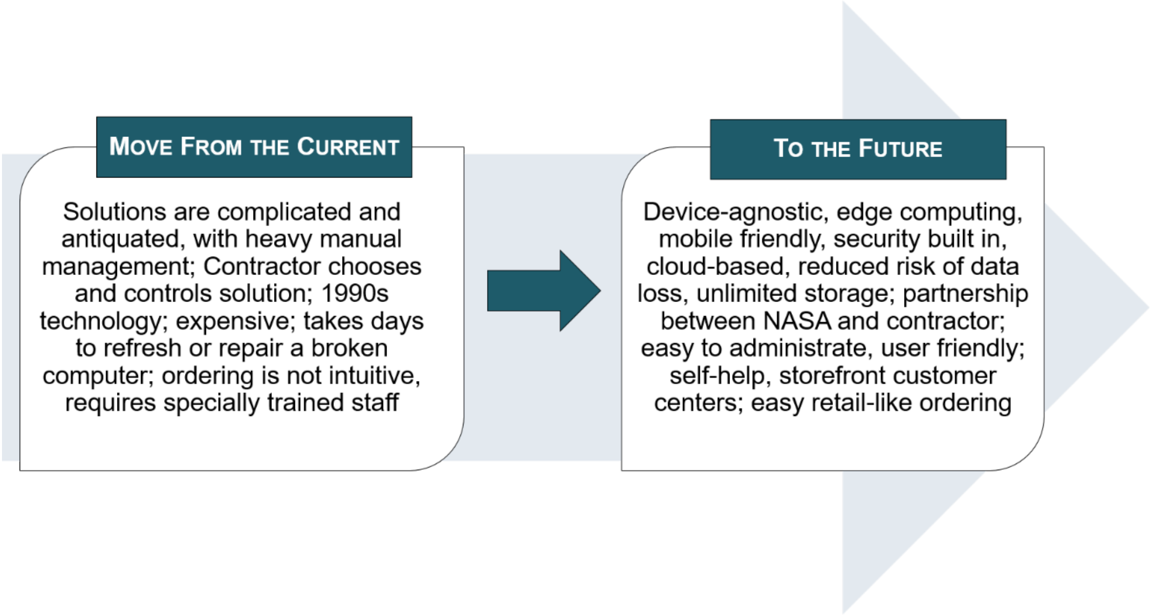
NASA has operated in the same inclusive seat-based model for almost two decades. While it initially served Agency objectives well, this model has become outdated due to the rapid changes in the IT industry. NASA is seeking to catch up and stay abreast of those changes in the IT industry, and is pursuing a partner that can contribute to the innovation required to move NASA to the current state-of-art and then forge ahead with new opportunities as industry paradigm shifts present themselves. To realize this vision, NASA expects its partner to employ modern techniques to achieve the goals and objectives referenced in this document while supporting the NASA workforce in a device-agnostic, mobile friendly environment with built-in security and cloud based resources. In addition to state-of-the art solutions, NASA's workforce desires the ability to request end-user services and retail-like catalog orders. The development of a strategic partnership is critical to NASA's successful transformation of the current end-user experience and to providing the necessary agility to support its diverse workforce in the execution of Agency missions.

NASA has already started the transformation. NASA has acquired Office 365 licensing and is starting the implementation project; NASA has an enterprise file sync and share (EFSS) pilot underway, and a pilot project working on virtualization solutions. NASA will transform from its current state to its intended future state and is seeking an innovative Contract partner to support this transformation journey.



NASA desires to transform the status quo—especially in the End-User compute services element of the contract. NASA wants to move beyond the current seat-based structure to adopt more modern computing methodologies, and envisions a secure edge computing model similar to eBanking. PWS section 1.2 states many of the objectives we seek to achieve. NASA requests potential Contractors to evaluate NASA's objectives and recommend how Contractors would partner with NASA to achieve them.

NASA is looking to develop a strategic partnership to transform the end-user experience to provide the necessary agility to support its diverse workforce and mission. The types of support needed for the end-user services program could include (but are not limited to) enterprise architecture, desktop engineering, project



Move From the Current

Solutions are complicated and antiquated, with heavy manual management; Contractor chooses and controls solution; 1990s technology; expensive; takes days to refresh or repair a broken computer; ordering is not intuitive, requires specially trained staff

To the Future

Device-agnostic, edge computing, mobile friendly, security built in, cloud-based, reduced risk of data loss, unlimited storage; partnership between NASA and contractor; easy to administrate, user friendly; self-help, storefront customer centers; easy retail-like ordering management support, transformation and operation support, continual service improvement and communications, and other program support functions.

The Contractor shall:

a. Develop a defined roadmap for EUSO based on guidance from NASA. The Contractor shall recommend processes, procedures, governance strategies and propose rules and policies to implement the roadmap and identify risks and challenges to implementation, and provide a project plan(s), schedule and costs including recommended future service and device CLINs. The Contractor shall provide a plan within 120 days after effective date of the Contract.
b. Assist NASA in transformation from the current all-inclusive seat-based model to a new way of providing end-user compute services for NASA that is device agnostic and focuses on edge computing. NASA EUSO is currently using an all-inclusive seat-based model. Within 60 days of the resulting roadmap specified in 4.0.a, the Contractor shall develop a transformation model for a new way of providing compute services for NASA that is device-agnostic and focuses on edge computing. The hardware acquisition and software services will be separate CLINs in the transformation model. The plan will move NASA to role-based provisioning so that users are provided the device(s) and applications appropriate to their job duties—not "one size fits all." The Contractor shall recommend governance and propose rules and policies to implement a device-agnostic, role-based transformation model and identify risks and challenges to implementation, and provide a project plan, schedule, and costs including recommended CLINs.
c. Provide a detailed roadmap for desktop virtualization technologies that includes a range of use cases developed in collaboration with NASA, project timelines, and cost estimates including recommended CLINs, etc. within 60 days of the resulting roadmap specified in PWS section 4.0.a.
d. Develop a plan to migrate end-user data off the NEST and Government-owned end user devices and store it in NASA servers that are cloud-based (public or NASA Data Center) within 90 days of the resulting roadmap task specified in 4.0.a. The Contractor shall provide a range of use cases developed in collaboration with NASA, project timelines and cost estimates including recommended CLINs. The storage solution shall utilize the capability provided by NASA EFSS services as the first option. The Contractor shall partner with NASA to relocate end-user data off the local device to provide storage that is:
    - Quick to access – comparable to local drive data access
    - Cloud based is preferred and the long-term objective
    - Secure
    - Sharable
    - Searchable
    - Resilient
    - Accessible/available on all user's devices
    - Includes Digital Rights Management (DRM) capability including data tagging
    - Analytics capable
e. Partner with NASA to develop, prepare, and operate an Application Management site (app store) for NASA-approved COTS and in-house developed applications and software.
f. Work with ESD to develop end-user service requests in NASA's ITSM system that provide a user experience similar to retail entities. The Government's service request requirements

are defined in Section 6.3. The Contractor shall work with ESD during the transition period to transform the existing service definition process described in Section 6.3 into a process in which the Contractor takes ownership of the service definition process and only relies on ESD for system access, system support, and the NSSC change and release management process requirements to move the NEST service changes to the production version of NASA's ITSM System.

i. The existing process described in Section 6.3 requires the Contractor to submit service requests to the ESD development team, and to test the completed services before they go live.

ii. The new process to be developed during the transition period will require the Contractor to provide ServiceNow-certified developers who will create and maintain all NEST service definitions in an NSSC development instance of ServiceNow. NSSC will provision access to the system, and will respond to any system support issues. The NSSC Configuration Management process will govern these changes as they are developed and tested to ensure a working product is in place before any changes are moved into the production environment.

5.0 CYBERSECURITY MANAGEMENT

The integrity, confidentiality, and availability of NASA's IT systems and data is critical to accomplishing NASA's missions. NASA seeks a partner that will not only work toward hardening NASA's core IT Security posture, but will also develop innovative approaches to enhancing NASA's defenses without sacrificing the user experience. To that end, the Contractor shall:

a. Comply with the information security requirements as defined in NPDs, NPRs, NASA Interim Directives (NIDs), IT Security Handbooks, PDM, and NASA standards as identified in the Applicable Documents List cited in NFS 1852.204-76, *Security Requirements for Unclassified Information Technology Resources*.

b. Comply with the IT security requirements outlined in this PWS section both in managing the execution of the Contract, as well as the delivery of services to end users.

c. Consider the language in this PWS as authoritative for any IT Security requirements that are not explicitly cited in the applicable documents list referenced in NFS 1852.204-76, unless superseded by additions or updates to NASA policy documentation.

d. Identify an IT Security POC who will partner with NASA in order to ensure all systems within the scope of this Contract abide by the appropriate IT Security requirements and maintain the authority to operate while in service, and possesses sufficient authority to drive the necessary change to establish an effective IT Security program in execution of the Contract and in the delivery of services.

e. Obtain approval from the Senior Agency Information Security Officer prior to implementing and/or deploying any IT security services.

f. Submit their management approach for IT Security per Attachment I-2, DRD SM-01, *Information Security Management Plan*.

g. Provide a regular status of EUSO's state of IT Security via Attachment I-2, DRD SM-02, *IT Security Status Report.*

5.1 CYBERSECURITY FOCUS AREAS

While not a complete list of all IT Security requirements, NASA is highlighting the following IT Security requirements for managing the Contract and for fulfilling end-user services. Unless superseded by updates to policies, handbooks, Policy Decision Memoranda (PDM), or NASA standards as referenced in NFS 1852.204-76, the Contractor shall adhere to the following requirements.

5.1.1 Data Protection

The Contractor shall:

a. Comply with information protection requirements in accordance with NASA Privacy Policy and Procedural Requirements, and assess all information collections to ensure compliance with federal regulations and privacy protection requirements using the NASA-provided assessment tool, currently the Privacy and Controlled Unclassified Information Assessment Tool (PCAT).
b. Comply with FAR 52.224-1, *Privacy Act Notification* and FAR 52.224-2, *Privacy Act* clauses when the Contractor is required to design, develop, or operate a system of records on individuals to accomplish an Agency function, and ensure their employees comply with the requirements of the NASA Privacy Management Program.
c. Protect all sensitive information in accordance with NID 1600.55, *Sensitive But Unclassified (SBU) Controlled Information*, and the follow-on impending NASA Controlled Unclassified Information policy.
d. Protect all sensitive data with NASA-approved Federal Information Processing Standard Publication (FIPS PUB) 140-2, *Security Requirements for Cryptographic Modules* compliant solutions for data-at-rest (DAR) and data-in-transit.
    i. All information technology devices that store NASA data shall be encrypted using DAR per NASA IT Infrastructure Integration Program PDM 2013-127-EUS.
    ii. Provide solutions that encrypt sensitive information (e.g., SBU, Personally Identifiable Information (PII), Export Control) at the file and email levels.

5.1.2 Security Access and Authorization

The Contractor shall:

a. Comply with the access, authentication, and registration requirements as defined in NPR 2841.1, *Identity, Credential and Access Management* (ICAM), including:
    i. Manage user accounts for Contractor-managed IT systems and applications, including elevated privileges (EP) accounts, using the NASA Access Management System (NAMS).
    ii. Provide application authentication and authorization, including coordinating with the NASA Enterprise ICAM team to ensure that a NAMS asset workflow is established for each user-authenticated system and application managed by the Contractor.
    iii. Register applications using the designated NASA Application Tracking/ Registration system, currently the System for Tracking and Registering Applications and Websites, or its replacement.
b. Comply with OMB M-15-13, Subject: Policy to Require Secure Connections Across Federal Websites and Web Services.
c. Only use NASA IP address space when located at a NASA Center and shall not provide or allow any non-NASA internet connections under this Contract.
d. Comply with the Federal and Agency Internet Protocol version 6 (IPv6) transition utilizing guidance from:
    i. NASA Memo, dated March 21, 2016, Subject: Policies to Ensure IPv6 Compliance for Information Technology (IT) Purchases

   ii. OMB Memo, dated September 28, 2010, Subject: Transition to IPv6.

e. Ensure that appropriate IPv6 waivers are in place for any non-compliant hardware, software, or services acquired in the execution of this contract per guidance in the NASA IPv6 Compliance Users Guide.

5.1.3 Security Documentation

The Contractor shall:

a. Comply with the requirements for security authorization, also known as Security Assessment and Authorization (SA&A), of Contractor-managed information systems, consistent with FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* and NIST SP 800-37 (Revision 1), consistent with Attachment I-3, SLA SM-2. A NASA official, determined in accordance with NPR 2810.1A, *Security of Information Technology*, shall perform the role of the authorizing official for all such information systems.

   i. The Contractor shall support all SA&A activities on behalf of NASA information system owners (ISOs) and shall have an in-depth understanding and knowledge of the NASA and Federal policies, as well as the relevant NIST guidance, in developing compliant SA&A documentation.

   ii. For all information systems provided under this contract that store, process or transmit NASA data, the Contractor shall assist NASA ISOs and data owners in categorizing NASA information and information systems in accordance with NASA policy and with FIPS PUB 199 and NIST SP 800-60.

   iii. The Contractor shall support NASA ISOs in the development and maintenance of information system security documentation. SA&A documentation may include, but is not limited to, System Security Plans, Risk Assessment Reports, Security Assessment Reports, Contingency Plans, Authorization to Operate (ATO) documents, etc. All documentation shall be maintained in the NASA authoritative system for risk management and SA&A documentation (currently Risk Information Security Compliance System (RISCS)).

   iv. The Contractor shall support the definition of system boundaries, system hardware/software inventories, system interconnections, system responsible officials, and system users.

   v. The Contractor shall analyze the system and provide security control recommendations to the ISO in accordance with NASA policy and the current NASA approved/required revision of NIST SP 800-53.

   vi. The Contractor shall support all applicable security assessments of each information system. 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 the Inspector General (OIG) audits, Government Accountability Office (GAO) audits, and Agency-approved network penetration testing. The Contractor shall provide support in responding to data calls and requests for information related to such audit activities, and in developing formal and information audit responses. For example, the Contractor shall support the development of exhibits, artifacts, and reports, the analysis of findings and the tracking of corrective measures, as requested by NASA.

   vii. The Contractor shall document, track, and report risks and security vulnerabilities identified during the security assessment for each information system in RISCS and address or remediate vulnerabilities on a schedule as approved by the NASA authorizing official consistent with Attachment I-3, SLA SM-1 and SM-3.

viii. The Contractor shall perform continuous monitoring of the information system in accordance with NASA policies and shall support NASA ISOs in all activities surrounding continuous monitoring of the security of the information system and shall:

(a) Ensure that the results of continuous monitoring are reported appropriately in NASA's authoritative system for risk management and SA&A documentation.

(b) Ensure that continuous monitoring is an integrated component of risk management for the information system.

(c) Ensure the results of continuous monitoring are used effectively and efficiently to drive updates to system security controls and SA&A documentation.

b. Maintain appropriate NASA-approved contingency plans for any information systems, applications, services, and facilities managed by the Contractor on behalf of NASA. This includes training Contractor personnel and NASA personnel, as needed, on those contingency plans, and periodically testing/exercising those contingency plans, in accordance with Federal and NASA requirements, policy, and guidance. In the event that contingency plans are executed during an actual emergency, the Contractor shall:

i. Conduct emergency operations during a contingency event in accordance with developed and approved contingency plans.

ii. After a contingency event, ensure that operations of required information systems, services and facilities (including computers, networks, applications, data repositories, telecommunications, environmental, and technical support) can be resumed within required business timeframes.

5.1.4 System Vulnerability Management and Configuration

The Contractor shall:

a. Process and complete all request for Collection of Electronic Data (CED) in a professional and discreet manner in accordance with Attachment I-3, Service Level Agreements, SM-5, CED Process and Implementation.

b. Address all vulnerabilities of all information systems under the scope of this contract in accordance with NASA policy and guidelines as set forth in NPR 2810.1A and applicable IT Security Handbooks, including any organizationally defined values (ODV). All vulnerabilities from the manufacturers of the hardware, software, or firmware of the devices shall be addressed in accordance with Table 5.1.4-1, Vulnerability Remediation Timeline, by correcting the findings or presenting an Accepted Risk or a Plan of Action & Milestone (POA&M) to the AO for approval consistent with Attachment I-3, SLA SM-1 and SM-3. The vulnerabilities are reported from multiple sources, including: external reports, the NASA SOC Mitigation Action Recommendation (MAR) actions, Center vulnerability patch actions issued through the individual Center/NASA Facility action tracking process, and Federal/Agency/Center security assessments (Department of Homeland Security, Agency Network Penetration Test, Web Application Deep Dive, Web Application Security Project, regularly scheduled network vulnerability scans, GAO and OIG audits).

i. The following defines the current Agency standard timelines for remediation of vulnerabilities and the creation and management of POA&Ms as cited in ITS-HBK 2810.02-08, Security Assessment and Authorization: Plan of Action Milestones. The timeline is based on both the vulnerability rating and the FIPS PUB 199 categorization defined within the System Security Plan.

Table 5.1.4-1 Vulnerability Remediation Timeline

Vulnerability Rating	Remediation Timeline by Systems FIPS PUB 199 Security Categorization (in calendar days)		
	High	Moderate	Low
Critical	9	12	14
High	14	17	25
Medium	25	30	45
Low	45	55	70
SOC Expedited MARs	7	7	7

c. Scan all information systems provided under this Contract or used in support of this Contract for vulnerabilities (both credential and non-credential) in accordance with the NASA defined schedule and policy.

d. Perform all Agency-required vulnerability scanning, patching, application blacklisting and whitelisting, and reporting using the Agency's defined tool set necessary for these functions. Currently Microsoft's System Center Configuration Manager (SCCM) and Apple's Jamf Pro are used to push patches to end-user systems. CDM, RISCS, and ITSEC-EDW tools are used for vulnerability scanning, patching, and reporting vulnerability and patch status of end-user devices. NASA has not yet implemented application whitelisting utilizing CDM defined tools.

   i. Vulnerability and patch status reports from Agency CDM tools (Nessus and IBM's Big Fix) are the standards by which the contractor shall be held accountable for vulnerability and patching SLAs.

e. Obtain a NASA-approved waiver in accordance with NASA policy and procedures for any computing devices that cannot run the reporting agent software, and the Contractor shall manually report to NASA the results of vulnerability scans and remediation in accordance with NASA policies and guidance.

f. Propose a solution to transition from multiple patching tools to the Homeland Security defined CDM tools that are a part of NASA's CDM toolset.

g. Ensure that end-user systems are automatically rebooted on a regular basis to ensure patches are fully installed on systems, and shall also provide a deviation process with appropriate approvals when mission-essential functions would be adversely affected by automatic reboots.

h. Implement NASA ODV, as documented in NASA IT Security Handbooks, which provide NASA-specific required parameters for security controls defined in NIST Special Publication (SP) 800-53 (latest NASA-approved revision), *Security and Privacy Controls for Federal Information Systems and Organizations*.

i. Plan for and implement the full system development lifecycle maintenance and updates of assets and systems, including but not limited to:

   i. Near real time asset tracking and reporting from procurement to retirement in order to optimize the most accurate IT Security response and analysis,

   ii. Removal of retired systems from Active Directory and pertinent IT Security asset databases, consistent with Attachment I-3, SLA SACM-1.

   iii. End of Life and End of Support replacement strategy in accordance with NASA requirements.

    iv. Data sanitization for assets (compute, mobile, print) in accordance with NPR 2810.1, ITS-HBK 2810.11-02 *Digital Media Sanitization*, and NIST SP 800-64, *Security Considerations in the System Development Lifecycle*, consistent with Attachment I-3, SLA SM-4 and SACM-1.

j. Configure and maintain operating systems and software on all information systems provided under this Contract in accordance with Federal and NASA security configuration policies and guidance. The Contractor shall ensure all applicable IT systems, applications, and services are securely configured based on the security configuration standards defined by Agency Security Configuration Standards, to include:

    i. Ensuring the NASA-provided Continuous Diagnostics and Mitigation (CDM) solutions are installed and continue to function properly (based on NASA OCIO assessment) on all supported IT devices and integrated with the Agency reporting mechanisms, including RISCS and IT Security Enterprise Data Warehouse (ITSEC-EDW), which feeds the Department of Homeland Security's Federal Dashboard.

    ii. Complying with the RISCS and ITSEC-EDW reporting requirements, including security configuration profiles, patch management, hardware inventory, and software inventory. The CDM tools must be installed for reporting. For systems that cannot install CDM tools, a NASA-approved waiver must be obtained, and the devices must be manually inventoried and reported to the RISCS and ITSEC-EDW per NASA policy and procedures.

    iii. Applying appropriate minimal-level of system privileges based on the user role consistent with ITS-HBK-2810.15-01A, *Access Control*, ITS-HBK-2810.15-02, *Access Control: Managed Elevated Privileges (EP),* and other applicable IT Security Access Control handbooks.

k. Protect the end-user computing environment from all adverse effects of software that may be either intentionally or unintentionally introduced into the end-user computing environment by end users, while simultaneously optimizing end user functionality to meet organizational missions by proposing a capability that continues to limit user privileges at the operating system and yet provides the end user with the flexibility to utilize organizationally unique software necessary to perform work. This capability may be addressed by, but is not limited to, the following:

    i. Provide a capability for the Contractor to manage Government approved/whitelisted software installation and updates that permits the end user with self-service access to appropriate applications and updates, with the goal of utilizing or transitioning to the Agency standard CDM tool for application whitelisting, once available.

    ii. Provide a capability to allow end users (or designated noncontract system/application administrators) to install applications and updates without EP and without diminishing the security posture of the end user device.

    iii. Provide a service whereby the Contractor assumes management of organizationally unique applications by providing commercially available updates and all vulnerability remediation of on behalf of requesting NASA organizations.

    iv. Establish a virtualized environment for the end-user application that segregates potential vulnerabilities from the native end-user computing environment without significantly diminishing the performance, functionality, and interoperability with the core desktop software of the end users.

l. Protect all information systems using NASA enterprise anti-malware and other malicious code protection (including anti-virus and anti-spyware) solutions, which provide automated updates of malware/malicious code detection definitions at least once every 24 hours and automated logging and reporting.
    i. For any system that cannot use the anti-malware solution or for which no anti-malware software exists, the Contractor shall obtain a NASA-approved risk acceptance for continued operations in accordance with NASA policy and procedures.

m. Comply with the Agency Supply Chain Risk Management process, NFS 1852.239-74, Information Technology System Supply Chain Risk Assessment, and NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations by obtaining Government approval using NF-1701 before procuring any IT applications or systems, hardware or software, including all offerings in the Product Catalog.

5.1.5 Cloud-based Security

The Contractor shall:

a. Follow all relevant NASA IT Security policy and guidance related to cloud-based services delivered under this Contract. This policy and guidance includes, but is not limited to, the following:
    i. Ensuring that any cloud-based services provided has a documented ATO or interim authority to operate from the NASA authorizing official (AO).
    ii. Ensuring the appropriate FIPS PUB 199 categorization for cloud services, by identifying the information types that will be processed, stored, or transmitted.
    iii. Clearly defining and documenting information and system boundaries between cloud service providers and NASA infrastructure.
    iv. Any data flow crossing a boundary must be supported by an appropriate Interconnection Security Agreement, or Memorandum of Understanding.
    v. Ensuring all NEST Contractor-related cloud SA&A documentation is entered into NASA's RISCS system.
    vi. Implementing and managing appropriate NASA and Federally mandated technical and operational security controls, including the cloud service provider inheritance hierarchy.
    vii. Developing a continuous monitoring strategy and implementing a continuous monitoring program for cloud-based services, to include assessing security controls, assessing risk-based criteria, and developing agreements with cloud service providers to gain insights relative to their ongoing control assessment results and significant change management activities.
    viii. Providing continual visibility into cloud service usage via discovery capabilities.
    ix. Documenting and assessing all change events, including providing a Security Impact Assessment for significant changes.
    x. Performing an Initial Privacy Threshold Analysis/Privacy Impact Assessment using the PCAT for each application.
    xi. Assisting in the coordination between the SOC and cloud service providers when an IT Security incident relative to cloud services has been identified.
    xii. Reporting suspected privacy breaches in accordance with Federal requirements.

5.1.6 Incident Management

The Contractor shall:

a. Support the integration of NASA Security Operations Center (SOC) IT security services, technologies, and processes into systems and services provided under this Contract and in support of this Contract, in accordance with NASA guidance.

b. Follow NASA security incident management policies, processes, and procedures and ensure coordination of its incident response team with the NASA SOC, and shall promptly report to the NASA SOC any suspected security incidents (including unauthorized access) involving hardware, software, firmware, networks, infrastructure, or sensitive data occurring on any physical, virtual, or cloud-based systems. The Contractor shall provide all immediate and timely necessary assistance and access to the affected systems to NASA (SOC, EUSO, Field Centers, OCIO, OIG) so that a detailed investigation can be conducted, problems remedied, and lessons learned documented. The Contractor shall inform other NASA stakeholders as necessary, with guidance from the SOC, such as the ESD, the CSO, and mission related offices. Security logs and audit information shall be handled according to evidence preservation procedures.

c. Notify the SOC followed by the Chief Information Security Officer within one hour of discovery of an incident involving SBU, PII, and/or Export Control information.
Verbally notify the SOC within two (2) hours of incident discovery for all lost or stolen equipment. After verbal notification of loss or theft, an interim written report will be provided within twenty-four (24) hours of incident discovery to the EUSO per Attachment I-2, DRD IT-03, *Lost, Damaged, Destroyed and Stolen Property Report*.

d. Make available logs from any information system to the NASA common logging environment, as directed by the NASA SOC. Electronic raw log data shall be forwarded from the source device to the NASA common logging environment, in accordance with NASA policies, procedures, and guidance.

e. Provide a logging environment that centrally captures and retains logs from all information systems provided under this Contract.

5.1.7 Personnel Security and Training

The Contractor shall:

a. 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. In addition, system administrators shall not be granted EP to information systems covered under this Contract unless they are authorized and have met the training requirements in accordance with NASA policy.

b. Ensure that all Contractor employees successfully complete the mandatory NASA Information Security Awareness training by the designated due date.

c. Implement a comprehensive physical security program consistent with NASA and Center-specific regulations and procedures for the performance of the Contract and the protection of assets and equipment that process NASA data.

   i. At all times, the Contractor shall comply and ensure their employees comply with the requirements of the NASA Security Program. These regulations and procedures include NPR 1620.3, *Physical Security Requirements for NASA Facilities and Property*; NPD 1600.2x *NASA Security Policy*; and NPR 1600.1, *NASA Security Program Procedural Requirements,* ITS Handbook (ITS-HBK-2810.12-01*) Physical and Environmental Protection*.

6.0 SERVICE MANAGEMENT

The Contractor shall employ the Information Technology Infrastructure Library (ITIL) Service Management Framework (Version 3 and any subsequent revisions) to guide provisioning of the services, processes, functions, and other capabilities needed to support EUSO services. The Contractor shall provide restoration of services within this section per Attachment I-3, SLA IM-1, *Incident Resolution*.

6.1 TIER 0/1 SERVICE DESK

a. The Contractor shall support the ESD in first contact resolution (FCR). The ESD is the front end for NASA customers to access enterprise and Center/Mission Directorate (MD) IT and non-IT services. The ESD provides NASA customers with:
   - A 24/7 service desk for enterprise and Center/MD Tier 1 support
   - Online access to >3000 KAs, FAQs, training resources, and more.
   - Online access for submission and status of incident tickets for enterprise and Center/MD programs.
   - Online catalog for requesting and status of ~250 Enterprise and Center products and services.

   The guiding documentation for how NASA users interact with the ESD is found in NSCG-2800-0006, *Enterprise Service Desk (ESD) Tier 0 (Self-Service) Customer Guide*. Documentation for how the ESD supports NASA users is found in NSSDG-2410-0001, *Enterprise Service Desk Service Delivery Guide*. Both documents are included in the Bidder's Library. Additional details are provided in the sections pertaining to PWS section 6.4 Incident Management and 6.3 Service Request Management in this document.

6.1.1 Reserved

Reserved for Tier 0/1 Enterprise Service Desk Support if an Agency decision is made to move Tier 0/1 ESD support under NEST.

6.2 TIER 2 SUPPORT

The Contractor shall:

a. Provide Tier 2 support 24/7 with escalation paths to their Tier 3 providers. Tier 2 support may be physical or virtual.
b. Use NASA's ITSM system for responding and interacting with Tier 1 service desk, the ESD.
c. Provide Incident Management support by working directly in the NASA ITSM system.
d. Work directly with the ESD Organization at the NSSC as described by agreed upon ACAs and Operational Level Agreements (OLA).
e. Ensure that Tier 2 has escalation procedures in place for escalation of major incidents and incidents from VIP users.
f. Provide system expertise for all NEST services in troubleshooting, root cause analysis, and resolution of issues.
g. Work to minimize the number of times end users speak to an IT Technician by measuring, reporting, and improving upon its First Response Resolution (FRR) at Tier 2.

6.3 SERVICE REQUEST MANAGEMENT

The Contractor shall:

a. Provide service request fulfillment by working directly in the NASA ITSM system. When a request is approved by NASA, a fulfillment task will be assigned to the appropriate contractor(s). The contractor(s) shall update the task with status and completion information, and shall be required to provide fulfillment information on the affected asset record. (See NSCG-2800-0010, *Enterprise Service Desk Service Request Customer Guide* in the Bidder's Library for additional details regarding the service request process.)
b. Be held accountable to Customer Satisfaction response results defined in Attachment I-3, SLA SD-5, *Customer Satisfaction of Service Delivery*. Contractors shall use self-service reporting in the NASA ITSM system to view responses. ESD will assign tickets to Tier 2 whenever a customer requests contact or when they leave feedback that requires Tier 2 follow-up.
c. Ensure completion of services requests to customer's satisfaction per Attachment I-3, SLA SD-6, *Service Delivery Reopen Rate* and SD-5, *Customer Satisfaction of Service Delivery*.
d. Work with the EUSO to define the service definitions that appear in the NASA service catalog.
e. Work with the EUSO to define, test and validate service request automation for each service offered to NASA users in the service catalog. All service definitions are carried out directly in the NASA ITSM system. For details on the service definition process, please refer to NSSDG-2800-0001, *NSSC Service Definition Repository Service Delivery Guide* (see Bidder's Library). The Contractor shall work closely with the EUSO Service Delivery Manager to coordinate this process.
f. Provide service definition (plans for new definitions and for modifications) and request fulfilment issues as they occur as topics for the monthly operational meetings defined in PWS section 6.4, Incident Management.
g. Update assigned service requests to address request status, assigned group, routing, and any constraints to delivery of services.
h. Document causes of delays outside of the Contractor's control to support metric waiver requests in service request work logs.
i. Perform trend analysis per Attachment I-2, DRD IT-12, *Incident and Service Request Performance Report* on an ongoing basis to identify issues within the live environment.

6.4 INCIDENT MANAGEMENT

The Contractor shall:

a. Serve as the primary service provider for Tier 2 and higher support for all NEST provided services.
b. Provide Tier 2 support by working directly in NASA's ITSM system.
c. Support transformation at Tier 2 and higher levels to an ITIL-based incident prioritization methodology based on impact and urgency. The Contractor's approach to this transformation shall be detailed in Attachment I-2, DRD MA-03, *Phase-In Plan*.
    i. The Contractor shall work with ESD and EUSO to identify which activities, services, and functions are to be considered "critical," "major," "minor," or "small" to match the framework defined in Table 6.4-1.
d. Update assigned Incidents in NASA's ITSM system to address incident status, incident impact and urgency, assignment group, routing, and any constraints to the delivery of services.

Table 6.4-1: Priority Matrix

		IMPACT			
		1 - Extensive / Widespread	2 - Significant / Large	3 - Moderate / Limited	4 - Minor / Localized
URGENCY	Critical	P1	P1	P2	P2
	High	P1	P2	P2	P3
	Medium	P2	P3	P3	P3
	Low	P4	P4	P4	P4

e. Document causes of delays outside of the Contractor's control in incident work logs to support metric waiver requests.

f. Reroute incidents received by the Contractor that are not within the Contractor's scope of work to the ESD noting any all research, findings, and customer interactions performed to permit proper further routing of the incident.

g. Perform, as a joint effort between EUSO, NEST, and the ESD, analysis of NEST related incident tickets to support proactive identification of and quick reaction to issues in the environment per Attachment I-2, DRD MA-01, *Management Plan*. The Contractor's analysis shall include tickets resolved at the FCR (ESD) level.

h. Perform trend analysis per Attachment I-2, DRD IT-12, *Incident and Service Request Performance Report* on an ongoing basis to identify issues within the production environment in order to identify:

    i. NEST related incidents that have not occurred on a repetitive basis enough to warrant escalation to a Problem ticket, but have occurred enough to warrant a potential issue or degradation within a service or product.

    ii. Any issue within a process that would require a review to correct the process or address adherence to the process.

    iii. Any warrant for the creation of a KA, Agency communication, and/or discussion/training with the ESD to improve first contact resolution.

    iv. Any change in end user behavior/actions that would require EUSO to address acceptable use policies.

i. Follow NASA IT Security incident processes for all incidents categorized as an IT Security incident and ensure that incident resolutions do not impact IT Security investigations.

j. Serve as a primary stakeholder and lead within the Major Incident Response activities for EUSO provided services and shall be responsible for the coordination of stakeholder attendance, troubleshooting, documenting, and resolution implementation.

k. Refer to Attachment I-3, *Service Level Agreements (SLAs)* for metrics associated with ticket priorities, and shall always consider Incident response for VIP users a Priority 1 ticket.

l. Be held to Customer Satisfaction results defined in Attachment I-3, SLA IM-3, *Customer Satisfaction*. The Contractor shall use self-service reporting in the NASA ITSM system to view responses and address missed SLAs as required. ESD will send customer satisfaction surveys for 100% of incidents marked "Resolved," with the following exceptions:

- Status Inquiries
- Tickets referred to Center or another service desk
- Tickets marked as duplicates

ESD will assign tickets to Tier 2 whenever a user reopens a ticket that the Contractor has marked Resolved. ESD will also assign tickets to Tier 2 whenever a customer requests contact or when they leave feedback that requires Tier 2 follow-up.

m. Prevent premature closure of Incident Tickets per Attachment I-3, SLA IM-2, *Incident Reopen Rate*.
n. Participate in monthly operations meetings with Government contractors with which the NEST Contractor holds an ACA, as identified in the Model Contract section 6.10, Associate Contractor Agreements, regarding NASA OCIO operations and as needed in order to assure integration of issues and open work. The NEST Contractor shall facilitate, lead, and participate in meetings at the request of the EUSO. Additional impromptu meetings will be required to support Event, Incident, and Problem Management.

6.4.1 Incident Response for Teleworkers, Travelers, and Off-Site Users

The Contractor shall:

a. Ensure that telecommuters (i.e., end users who work from a remote location), travelers (end users at a NASA or non-NASA temporary duty location), and other off-site end users (see Table 1.5-1, NASA Service Performance Sites) experience minimal interruption of services at the remote location for services within the Contractor’s scope. SLAs defined in the Contract shall apply to remote users.
b. Provide, at a minimum, incident support by shipping properly configured hardware and software to the end user using drop ship methodology or other COR-approved method when the end user needs incident support that cannot be provided remotely.
c. Provide the shipping materials, including packaging. The Contractor shall be responsible for all costs associated with shipping and material handling.
d. The Contractor shall provide maintenance support for travelers at NASA Centers regardless of the user’s home Center.

6.5 KNOWLEDGE MANAGEMENT

The Contractor shall:

a. Create, review, maintain, and monitor KAs required to support all NEST services, ESD initial troubleshooting, ESD FCR, and ESD Self-Help.
b. Ensure KAs are identified and created to support a seamless transition from project state to production as a part of the Contractor’s participation in project initiatives.
c. Coordinate with EUSO and other service offices/contractors to ensure the accuracy of NEST-provided KA content for services as they relate to services provided by another service office.
d. Ensure Contractor staff are cross-trained to a level of knowledge required to complete IT services requests and incidents.
e. Ensure all KAs are maintained and updated for all NEST supported services as changes to End User Services occur.
f. Manage NEST related KAs in accordance with ESD KA SOP NSCG-2800-0009, *ESD Knowledge Management Customer Guide* (see Bidders Library).

6.6 SERVICE ASSET AND CONFIGURATION MANAGEMENT (SACM)

For all NEST service assets, the Contractor shall:

a. Provide and execute a plan for management of NEST service assets per Attachment I-2, DRD MA-11, *Service Asset and Configuration Management (SACM)*.

b. Mark all non-consumable service assets with the contract number, owner, and unique asset identifier.
c. Manage and track the complete lifecycle of service assets and their configuration from procurement to disposal in NASA's ITSM system.
d. Provide the Configuration Status Accounting (CSA) information within the NASA ITSM system to permit association of services by user, organization, Center, funding code, and location.
e. Associate service assets with ITIL processes (e.g. Service Requests, Incidents, Problems, Changes).
f. Update asset statuses, associations, and configurations as service assets are added, removed, modified, or replaced per timeliness requirements in Attachment I-3, SLA SACM-1.
g. Provide device accounting in NASA's ITSM system to include the following minimum fields:
    i. Deployed Status (e.g. In use, Available for deployment, Disposed)
    ii. Service Identifier (If associated with active service)
    iii. Request number
    iv. Unique asset identifier affixed to device
    v. Serial Number
    vi. Manufacturer
    vii. Model
    viii. Hostname
    ix. Operating System
    x. MAC Address
    xi. International Mobile Equipment Identity (IMEI) number
    xii. Location
    xiii. Assigned user
    xiv. Assigned user UUPIC
    xv. Assigned User Organization
    xvi. Configuration revision per DRD IT-07, *Vendor Product Performance Specifications*, in place at time of deployment
    xvii. Configuration per DRD IT-13, *Software Load Configuration*, in place at time of deployment
    xviii. Install date per current service association
    xix. Initial Install Date
    xx. Refresh Cycle
    xxi. Refresh Date
    xxii. Acquisition Cost
    xxiii. Asset Transition Value (to be automatically calculated based on Deployed Date, Refresh Date, and Acquisition Cost)
h. Participate in quarterly audit activities to ensure the accuracy of documented asset information.
i. Implement corrective actions to remediate discrepancies in service asset data.
j. Assume responsibility for configuration control (CC) of the hardware and software product baselines for each service offering.

k. Document/store all baselines, deviations, waivers, and assets delivered in a Government approved CSA database, and review the data and assure its accuracy.
l. Identify configuration items CIs for the Functional Baseline (system specification) and Product Baselines (Associated Parts List and Software Configuration Items) associated with each service offering. The Contractor shall define a hierarchical identifier for each CI and document the interface between the CIs.
m. Submit to a Functional Configuration Audit (FCA), a formal examination of the as-built configuration of the CIs against the service design documentation. The completion of the audit will establish the Product Baseline. Any changes to the Product Baseline will be processed by the End User Services Program CCB.

6.6.1 SACM Development

With the approval of and coordination with the EUSO, the Contractor shall:

a. Design, implement, and maintain an ITIL-based Service Asset and Configuration Management (SACM) System, Plan, and Processes to cover all of NASA's end-user assets. The SACM System shall be designed through the identification, definition, and management of CIs, controls, lifecycle status accounting operating procedures, and configuration management databases (CMDBs) comprised of Government-owned and Contractor-owned data sources.
b. Define a configuration management system (CMS) to include all Agency new and/or modified hardware, firmware, software, infrastructure, peripheral equipment used to deliver end-user services.
   i. Develop the CMS in the NASA ITSM system.
   ii. The CMS shall track, manage, and make available all SACM information including CIs and CMDBs.
   iii. The Government shall determine the official system of record for the SACM system including all CIs stored within the CMDBs.
   iv. Design the CMS and any related management or maintenance processes to provide a logical representation of asset and configuration data obtained from one or more physical CMDBs.
   v. CMDBs shall be comprised of Government-owned and Contractor-owned data sources.
   vi. All changes to the CIs shall be governed by NASA's EUSO Change/Configuration Control Board (CCB) and are subject to its program standards, processes, and procedures.

6.7 CHANGE MANAGEMENT

The Contractor shall:

a. Prepare and execute a Change Management process that complements the EUSO Change Management process as defined in EUSO SOP-ST-1200, *EUSO Change Management Process (CMP)*.
b. Use NASA-approved tools for initiation and management of change requests in the Change Management process.
c. Provide a Change Management process on the effective date of the Contract.
d. Include the following in the Change Management process:
   i. Define approach to identifying and classifying changes.
   ii. Define approach for independent testing and formal evaluation of change.

iii. Define Change Advisory Board (CAB) and emergency CAB.
iv. Identify approach to eliminating unauthorized changes.
v. Define tracking and management of change requests.
vi. Define approach to interfacing Change Management with Problem and Incident Management processes.
vii. Define approach to measuring and reporting change success, using NASA's authoritative source.
viii. Define approach for supporting NASA mandatory configuration freezes during which no updates or upgrades can occur to identified systems.
ix. Define approach for identifying areas for improvement in change management.
x. Define approach for Change Evaluation that evaluates the effect of the change, identifies risks, and determines if the change is ready to be implemented into the NASA environment.

6.8 SERVICE VALIDATION AND TESTING

The Contractor shall:

a. Prepare and submit a Test Management Plan per Attachment I-2, DRD MA-10, *Release and Deployment Management (RDM) Plan* that complements the EUSO test management process as defined in EUSO SOP-ST-1201, *EUSO Test Management Process*.
b. Use NASA-approved tools for initiation and management of test processes in Test Management.
c. Provide a Test Management process per Attachment I-2, DRD MA-10, *Release and Deployment Management (RDM) Plan.*
d. Include the following in the Contractor Test Management process:
    i. Define approach for planning, managing, controlling and reporting test activities to ensure any new services or changes to existing services are compatible with the NASA environment.
    ii. Define approach for scheduling and performing test activities. This includes internal testing, beta testing, pilot testing, and Early Adopter testing (initial deployment to a limited group).
    iii. Define approach for validating all test activities are complete.
    iv. Define approach for designing and verifying test models to minimize risk. Tests are carried out using manual or automated testing techniques and procedures.
    v. Define approach for evaluating exit criteria and reporting and registering all test results, comparing actual results with projected results.
    vi. Define approach for ensuring the integrity of the test environment.
    vii. Define approach for identifying areas for improvement in test management.
    viii. Define approach to develop and maintain a virtual test environment to provide testing of NEST provided services.

6.9 RELEASE AND DEPLOYMENT

The Contractor shall:

a. Prepare and submit a Release and Deployment Management Plan per Attachment I-2, DRD MA-10, *Release and Deployment Management (RDM) Plan* that complements the EUSO Release and Deployment Management process as defined in EUSO SOP-ST-1202, *EUSO Release and Deployment Management Process*.

b. Use the NASA ITSM system for initiation and management of release and deployment processes in Release and Deployment Management. The Contractor shall provide a Release and Deployment Management process in accordance with Attachment I-2, DRD MA-10, *Release and Deployment Management (RDM) Plan*.

c. Provide service lifecycle management of all NEST-provided services which shall encompass requirements management, software architecture, software procurement, software license management, software testing, software change management, configuration management, continuous integration, project management, and release management in accordance with Attachment I-2, DRD MA-10, *Release and Deployment Management (RDM) Plan*.

d. Include the following in the Contractor Release and Deployment Management process:

    i. Define approach for planning, scheduling, testing and deploying releases to deliver new and changed services while protecting existing services.

    ii. Define approach for planning the Release and Deployment that clearly defines the release and how it will be deployed.

    iii. Define approach for building and testing the release that includes standard procedures and templates.

    iv. Define approach for effective deployment of new and changed services into the NASA environment.

    v. Define approach for reviewing and closing out deployment.

    vi. Define approach for identifying areas for improvement in release and deployment management.

6.10 PROBLEM MANAGEMENT

The Contractor shall:

a. Design and implement, with the approval of and coordination with EUSO, an ITIL-based Problem Management process that outlines the actions and workflow for managing an enterprise-level Problem Management program.

b. Include a detailed workflow for the integration into other Service Management processes (i.e., Change Management, Incident Management, Event Management, and Configuration Management).

c. Provide a detailed plan for identifying, tracking, and continuous engagement to address Problem tickets.

d. Ensure focus on problems within the production environment which creates an adverse work experience for the end user.

e. Coordinate with EUSO to implement controls at the ESD level that feed into the continuous identification of problems.

6.11 CAPACITY MANAGEMENT

The Contractor shall:

a. Design and implement, with the approval of and coordination with EUSO, an ITIL-based Capacity Management Plan per Attachment I-2, DRD MA-12, *Capacity Management Plan.*

b. Design and implement, with the approval of and coordination with EUSO, an ITIL-based Capacity Management process that outlines the actions and workflow for managing an enterprise-level Capacity Management program.

6.12 AVAILABILITY MANAGEMENT

The Contractor shall:

a. Design and implement, with the approval of and coordination with EUSO, an ITIL-based Availability Management Plan per Attachment I-2, DRD MA-13, *Availability Management Plan.*
b. Design and implement, with the approval of and coordination with EUSO, an ITIL-based Availability Management process that outlines the actions and workflow for managing an enterprise-level Availability Management program.
c. Include a detailed workflow for the integration into other Service Management processes (e.g., Service Level Management, Incident/Problem/Service Request Management, Capacity Management, Change Management, Continuity of Operations, Security Management, and Identity, Credentials, and Access Management).
d. Ensure product supply chain, service, and resource availability reactively and proactively to ensure availability during temporary peak service demand periods.
e. Provide temporary end-user computing, mobile and print services to meet end-user needs with finite requirement timeframes.
f. Document the proposed management approach for risk reduction measures and recovery options to maintain service availability per Attachment I-2, DRD MA-06, *IT Service Continuity Management (ITSCM) Plan*.

6.13 EVENT MANAGEMENT

The Contractor shall:

a. Design and implement, with the approval of and coordination with EUSO, an ITIL-based Event Management process that outlines the actions and workflow for managing an Enterprise-level Event Management program.
b. Provide situational awareness (SA) of services in near real-time in order to interpret events, possible incidents, and problems; understand their operational impact; and decisively and rapidly take action to restore services and protect information on the NASA environment.
c. Ensure the Event Management process is fully integrated into all the ITIL Service areas within the contract and that appropriate actions are taken to adhere to these other ITIL processes.
d. Maintain ownership of the event throughout the event management lifecycle for services which the NEST Contract provides and will ensure appropriate events are detected, filtered, analyzed, correlated, and categorized to support the assignment of control actions for the given event condition.
e. Utilize the NASA ITSM system for Event Management and will coordinate with Enterprise Service Desk on the build out, implementation, configuration, and sustainment of NEST assets and services within the NASA ITSM system to support a fully integrated and operational Event Management capability.

7.0 INTEGRATION

The EUSO is responsible for integration across the entire portfolio of services and capabilities associated with the end-user services domain and IT lifecycle that includes strategy, planning and resourcing, execution, operations, and continuous improvement.

The Contractor shall be responsible for integrating throughout the entire IT lifecycle as it relates to services and products it provides.

a. The Contractor shall be responsible for linking, relating, and connecting a series of diverse existing processes, systems, services, and products spread geographically across the Agency produced by multiple manufacturers into data infrastructures and architectures in a coherent and unifying manner that links all the different systems, framework of applications, and support systems.
b. The Contractor shall execute the integration of services and products delivered by the NEST contract into the portfolio of services delivered by the EUSO and with services provided by or to other program offices.
c. In coordination with the EUSO, the Contractor shall partner with NASA to support integration and continuous improvement as it relates to NEST throughout the IT lifecycle as described below:
    i. Strategy – development of end-user service and product strategies; i.e., Agency needs, mission needs, evolving technologies, mandates, policy, etc.
    ii. Planning – service and process design, roadmaps, prioritization, tactical plans, business analysis, e.g. changes or integration as required.
    iii. Resourcing – budgeting and accounting for service provisioning, resource allocations.
    iv. Execution of new technologies and improved existing technologies – transition of services, project management, risk management, technical integration, service level management.
    v. Operations – operating procedures, execution of services, problem resolution, refreshes, performance measurements, problem resolution and existing services consumed by the end users or other IT delivery entities.

8.0 COLLABORATION AND MICROSOFT OFFICE 365 (O365) SERVICES

NASA seeks to offer services that facilitate efficient collaboration among end users. This section outlines the requirements in regard to those services. The Contractor shall:

a. Provide a detailed and thorough technical approach including PWSs, SLAs, and performance metrics for effective and efficient collaboration and messaging services.
b. Provide the following: collaboration and messaging services to support the sustaining operations of existing implementations, migration to already approved capabilities, and development and migration for future collaboration and O365 services.

8.1 OPERATIONS OF REMAINING ON PREMISE INFRASTRUCTURE

This section outlines the requirements regarding the maintenance and operations of remaining on-premise infrastructure. The Contractor shall:

a. Operate, maintain, and provide user support for the NOMAD services and capabilities including:
    i. Email
    ii. Directory and Resource Administration (DRA) and Group Policy Administration (GPA)
    iii. NOMAD Backup
    iv. NOMAD Retention Management
    v. IP Black Listing

vi. Antivirus for Exchange
vii. Large File Transfer
viii. Virus and Vulnerability Remediation

b. Operate, maintain, and provide user support for Skype for Business.
c. Manage operations, including critical software updates and patches to ensure compliance with NASA and Federal cybersecurity requirements Critical software updates include security updates, updates required to maintain vendor support, and updates required for operational stability.
d. Provide system administration capabilities to ensure operations and maintenance of Active Directory Services, Infrastructure, Capabilities, and Security Management.
e. Adhere to the EUSO change management processes.
f. Make recommendations for incremental improvements to legacy systems that are aligned with the long-term O365 implementation for Government consideration.
g. Decommission legacy systems as instructed by the Government.
h. Deliver services per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service*.
i. Provide restoration of service per Attachment I-3 SLA IM-1, *Incident Resolution*.
j. Provide NOMAD reporting in accordance with Attachment I-2, DRD IT-10, *NOMAD Services Reports*.
k. Assist the Government in creating and saving ad hoc reporting capabilities of NOMAD service levels and performance metrics.

8.2 NASA'S O365 IMPLEMENTATION AND MIGRATIONS TO NEW CAPABILITIES

To facilitate the implementation and operations of O365, and migration to new capabilities, the Contractor shall:

a. Assist the Government (including support contracts for other OCIO service areas and programs) in providing collaboration services that facilitate the overall implementation and integration of O365 applications and features that are aligned with the Government's mission objectives and enterprise architecture.
b. Provide development, maintenance, and system support for O365 services on a variety of platforms (PC, Mac, Linux, etc.), per Government requirements. Support includes maintaining any system's infrastructure framework, which has been integrated with other computer infrastructure components such as networking, storage, and authentication and authorization services.
c. Adhere to the EUSO change management processes.
d. Provide the functional support knowledge and subject matter expertise required to maintain and support O365 Enterprise Suite over the life of this contract. Functional support knowledge and subject matter expertise shall include knowledge of application functional configuration; functional integration of applications; the skills and abilities required to analyze and troubleshoot problems and inconsistencies across O365; and support for O365 online cloud presence.
e. Provide SLAs and performance metrics to measure the effectiveness and efficiency of Contractor performance.
f. Help coordinate cybersecurity incidents and ongoing investigations between the O365 vendor and the Government.

8.2.1 Operations

To facilitate the operations and maintenance of O365, the Contractor shall:

a. Provide O365 support that includes the full range of lifecycle management system engineering, development, testing and implementation services, as needed and as directed by NASA, to provide effective and efficient operations of the O365 platform. These efforts will be comprised of technical services, system and software development efforts, related IT engineering support, and testing capability within the defined service areas.
b. Support operations activities including: monitoring and managing O365 systems, investigating and resolving system issues, documenting issue causes and resolutions, and providing technical assistance to end users.
c. Operate, maintain, and support the following capabilities in O365: Exchange, Exchange Online Protection, OneDrive for Business, SharePoint Online, and Office Online.
d. Maintain all configurations items required for the effective and efficient operation of O365, Active Directory, and associated add-on applications and plug-ins.
e. Ensure execution of patching and updates of O365 Desktop Applications.
f. Adhere to established EUSO processes for change in configuration and change in the configuration management databases(s).
g. Operate future features of O365 as defined by NASA EUSO.
h. Create and maintain change request(s) to improve the efficiency and effectiveness of ordering, maintaining, and operating O365 and associated add-on and ancillary software (i.e., Active Directory).
i. Provide capability of enabling features of O365 by individual user, group, Center, or Agency.
j. Maximize automatic provisioning of services.
k. Manage or assist the Government in the transition of new and approved O365 environment features and application and infrastructure components into an operational state.
l. Assist the Government in the migration of NASA users and associated services to O365 as required.
m. Provide knowledgeable functional support resources to manage the interaction with third-party add-on applications as defined by NASA.
n. Ensure all O365 updates and enhancements are tested in a separate environment from the production environment and are approved for release in accordance with the EUSO change management and release management processes.
o. Provide access for the Government to perform testing verification and validation.
p. Document and provide support for O365 technical training to NASA users.
q. Provide instructions to other technical employees (e.g., system administrators, etc.) and descriptions of functionality to end users and NASA trainers. For example, the Contractor may provide information to be utilized in Computer Based Training, Classroom Training, Distance Learning Training, and any other training method that NASA employs.
r. Create or update end-user procedures, job aids, and/or training materials as needed to enable effective and efficient implementation and use of O365 feature and capabilities.
s. Provide release management for O365 features, software updates, and patches.
t. Provide O365 rule and policy development, testing, and reporting using the O365 admin console to support administrative features such as records management, privacy information, export control, and International Traffic in Arms Regulations (ITAR).
u. Support legal holds for e-discovery requests.

v. Deliver services per Attachment I-3, SLA SD-2, *Completion of Change to New or Existing Service*.
   Provide restoration of service per Attachment I-3, SLA IM-1, *Incident Resolution*.
w. The Contractor shall provide O365 reporting in accordance with Attachment I-2, DRD IT-11, *O365 Services Reports*. The Contractor shall propose service level agreements and performance metrics.
x. Assist the government in creating and saving ad hoc reporting capabilities of O365 service levels and performance metrics.

8.3 FUTURE IMPLEMENTATIONS

In regard to future implementations of collaboration services, the Contractor shall:

a. Assist the Government (including support contracts for other OCIO service areas and programs) in providing solution and application architecture services that facilitate the overall implementation and integration of O365 applications and features, as well as other messaging and collaboration services that are aligned with the Government's mission objectives and Enterprise Architecture.
b. Assist the Government's functional and technical SMEs to define the business and technical requirements for future messaging and collaboration implementations.
c. Assist the Government in the development of rough order of magnitude estimates for technology investments and implementation of future messaging and collaboration services including third-party add-ons as directed.

9.0 INFRASTRUCTURE OPERATIONS

The Contractor shall:

a. Provide all necessary data center services (e.g., servers, operating systems, and system administration) required to deliver the NEST services.
b. Ensure that all non-cloud based infrastructure is housed only in NASA data centers.
c. Ensure that the provisioned data center services provide the appropriate security controls for the system requiring those services.
d. Operate NASA's client management tools to support devices and software managed by the NEST Contractor and support increasing EUSO responsibilities for management of end-user computers, print, and mobile devices within NASA.
e. Provide required software licensing, subscriptions, and hardware infrastructure required for delivery of solutions unless otherwise specified in Attachment I-11, *List of Government Furnished Property*, Attachment I-4, *Government Provided Facilities*, Attachment I-25, *List of Licenses*, or otherwise specified to be provided by the Government.
f. Maintain existing systems and support implementation of new NASA IT systems via innovative approaches or technologies to meet NASA goals and objectives.
g. Perform operations and maintenance activities to modify systems or components, correct faults, improve performance, or adapt to a changed environment.
h. Ensure that any infrastructure components are refreshed or upgraded to address changes to service dependencies.
i. Refresh all physical infrastructure on a 60-month refresh cycle, or migrate to non-physical virtual or cloud infrastructure.
j. Document plan for refresh or migration to non-physical virtual or cloud infrastructure in Attachment I-2, DRD IT-04, *Technology Refresh Plan*.

k. Ensure availability of systems per Attachment I-3, SLA ITSM-1.
l. Report Infrastructure Asset Transition Value per Attachment I-2, DRD IT-06, *Infrastructure Asset Transition Value Report*.

9.1 DOMAIN ADMINISTRATION

The NEST Contractor will be granted delegations required to operate systems for which the Contractor is accountable. Management of NASA's Active Directory infrastructure is otherwise not in the scope of this Contract. The Contractor shall leverage the infrastructure for the sole purposes of managing their devices and services.

9.2 SOFTWARE MANAGEMENT

NASA software management policies and procedures are maturing, and NASA requires a partner to advise and assist in implementation of the evolving future state. The Contractor shall:

a. Provide software lifecycle management (SLM) for designated enterprise-wide end-user computing software.
b. Provide full product lifecycle management of computer software which shall encompass requirements management, software procurement, software license management, software testing, software change management, configuration management, continuous integration, project management, and release management in accordance with Attachment I-2, DRD MA-10, *Release and Deployment Management (RDM) Plan*, NID 7150.113, *Software License Management,* and NPR 7150.2x *NASA Software Engineering Requirements*.
c. Coordinate and configure usage of existing and future NASA's software management tools to facilitate software distribution for services in PWS section 10.2, Managed Software Services.
d. Perform software patching and reporting as specified in PWS section 5.1.4.
e. Configure NASA's software management tools to facilitate end-user software distribution and management by non-NEST application owners and system administrators.
f. Assist NASA in identifying additional opportunities for addressing NASA's software needs via addition to NEST Contract for management.

Current software management tools can be found in Attachment I-25, *List of Licenses.*

9.3 RESERVED

9.4 DATA-AT-REST ENCRYPTION/KEY ESCROW

The Contractor shall:

a. Operate NASA's data-at-rest (DAR) Whole Disk Encryption toolset to protect NASA data on Contractor-deployed systems as well as those provisioned by NASA and other NASA contractors.
b. Provide monitoring of Whole Disk Encryption of all Agency devices.
c. Remediate non-compliant systems for which the Contractor is responsible per subscription to Managed Software Services.
d. Provide Key Escrow services for key recovery, including systems for which the Contractor is responsible as well as other Agency systems that utilize the DAR solution.
e. Enable the ESD to perform key recovery at first contact resolution.

Current tools utilized for DAR encryption can be found in Attachment I-25, *List of Licenses.*

9.5 BACKUP AND RESTORE

The Contractor shall:

a. Operate NASA's end user compute device backup and restore capabilities, and assist NASA in preventing and recovering from data loss.
b. Provide reporting of backup status for all NEST systems per Attachment I-2, DRD IT-09, *Data Backup and Restore Services Report*.
c. Restore data at NASA request to support investigations or e-Discovery requests.

Current backup tools are documented in Attachment I-25, *List of Licenses*. Backup and restore solution is limited to end-user computing operating systems Windows, MacOS, and Linux. However, scope may expand to address mobile operating systems such as Android and iOS, and/or end-user computing and mobile devices provided outside of NEST services.

9.6 IT SUPPORT REMOTE CONNECTIVITY

The Contractor shall:

a. Operate and maintain remote connectivity toolsets to permit remote administration and assistance.
b. Provide client licenses and remote support connectivity for ESD agents to access NEST managed systems for the purposes of incident response and improved first contact resolution.
c. Ensure remote management capability is maintained through contract transition.

Current tools utilized for remote management can be found in Attachment I-25, *List of Licenses.*

9.7 MOBILE DEVICE MANAGEMENT

The Contractor shall:

a. Manage, operate, and maintain the existing MDM service, which is based on IBM Maas360, integrated with a NASA front-end registration service to provide PIV-derived user authentication certificates and PIV-S/MIME encryption certificates for secure email.
b. Continually research commercial advances in vendor-provided MDM solutions such as, but not limited to, Apple's Device Enrollment Program, Samsung's Knox capability, and Microsoft's InTune product for applicability to managing NASA's mobile and end-user compute devices.
c. Advise, architect, and upon NASA approval, implement the most technically beneficial and cost-effective solutions for NASA to securely manage mobile devices within the NASA environment.

9.8 PRINT INFRASTRUCTURE

The Contractor shall:

a. Operate NASA's Print Management infrastructure. The incumbent contractor currently operates local print servers at NASA Centers.
b. Provide for automatic print driver installation on all supported clients where required for printer utilization.
c. Configure printer infrastructure to support PIV-enabled secure printing.
d. Integrate printer infrastructure with NASA's Active Directory.
e. Enforce naming standards to aid in device identification.
f. Enforce security protocols.

g. Limit access to print devices, at NASA request, to a selection of users.
h. Create Print queues to enabled delivery of fully functional solutions per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery.*
i. Modify, and maintain print queues per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service*.
j. Provide roadmaps to address transformation requirements for cloud and mobile printing.

9.9 TWO-FACTOR USER AUTHENTICATION SERVICE DISTRIBUTION

The Contractor shall:

a. Provide Registration Authority functionality for the issuance of user authentication credentials and signing, encryption, and SSL/TLS (Web-based) certificates (excluding PIV Smartcard credentials).
b. Provide the distribution of two-factor authentication hardware tokens (e.g., RSA SecurID tokens).
c. Verify end-user identity information in accordance with NASA policy (using the NASA Registration Practice Statement) prior to issuing encryption, signing, and SSL certificates, hardware tokens, or other requested credentials.
d. Maintain and control inventory to ensure availability of Government-furnished hardware tokens.
e. Issue hardware tokens and certificates utilizing the NASA Identity Management and Account eXchange (IdMAX).
f. Distribute two-factor authentication hardware tokens to end users per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery*.
g. Assist end users with the activation of their hardware tokens and the management of the life cycle of all certificates (e.g., request, key recovery, PKCS#12, and Web certificates), including installation of software updates to support these certificates.

9.10 SERVICE OUTAGES

a. The Contractor shall minimize user impacts to maintenance activities.
b. The Contractor shall ensure availability of service enabling infrastructure per Attachment I-3, SLA ITSM-01, *Management Service Availability*.
c. The Contractor shall include as part of Attachment I-2, DRD MA-01, *Management Plan* an outage communications approach consistent with the EUSO Communications Plan.
d. The Contractor shall document the proposed management approach for establishing and maintaining ongoing recovery capability for IT services and their supporting components per Attachment I-2, DRD MA-06, *IT Service Continuity Management (ITSCM) Plan.*

9.10.1 Scheduled Outages

a. To be considered a scheduled outage, the Contractor shall communicate disruptions to NEST services in accordance with Attachment I-2, DRD MA-01, *Management Plan.*
b. The Contractor shall perform scheduled maintenance activities to prevent service disruptions during the business hours of 6:00 a.m. and 6:00 p.m., local time, Monday through Friday.

9.10.2 Unscheduled Outages

a. The Contractor shall notify the EUSO designee and affected users of unscheduled outages as soon as practical.

b. Unscheduled outages shall be reported per Attachment I-2, DRD IT-12, *Incident and Service Request Performance Report.*

10.0 END USER COMPUTING SERVICES

NASA requires flexibility in provisioning and management of end user compute (EUC) services. To provide flexibility in service offerings, NASA requires managed hardware and managed software services to be available separately. NASA anticipates that most users will subscribe to a bundle of services including hardware, software, and backup services to meet the needs of the end user. Customers who require diverse hardware that is not appropriate for enterprise offerings may elect to subscribe to only managed software services. Administrators of Government- or other non-NEST contractor-managed systems may offload backup responsibilities by subscribing to NEST backup services. The NEST EUC Subscription Service Model is represented by Table 10.0-1.

Table 10.0-1. NEST EUC Subscription Service Model.

Managed Hardware	Compute Hardware	Hardware reference configuration per NASA-STD-2805x and optional augmentations
	Included Hardware	Hardware and accessories required to be delivered with all compute hardware
	Optional Hardware	Hardware and accessories specified at time of service order or via changes though the life of the service
	Included Management Services	Requirements that apply to all managed hardware services
	Optional Management Services	Optional service specified at time of service order or via changes though the life of the service
Managed Software	Operating System	Operating systems as specified in NASA-STD-2804x
	Software Load	Software specified in NASA-STD-2804x and specified in Attachment I-25, *List of Licenses*
	Software Subscription by Title	Additional titles offered per monthly service
	Backup Services	Backup data resident on device

To deliver services within the NEST EUC subscriptions the Contractor shall:

a. Provide managed compute hardware services and managed software services in a subscription model in response to NASA requests for services submitted and approved via NASA's ITSM system.
b. Provide managed hardware services, managed software services, or combinations of both to meet NASA end-user requirements.
c. Remove services unsubscribed by NASA at no additional cost as requirements change.
d. Modify services as requested for elements specified as optional services.
Associate service assets to service requests in NASA's ITSM and update asset associations as service assets are added, removed, or replaced.
e. Manage EUC hardware and software per minimum specifications as defined in NASA-STD-2804x, *Minimum Interoperability Software Suite;* NASA-STD-2805x, *Minimum Hardware Configurations*; and Attachment I-25, *List of Licenses*, and as approved in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*.

10.1 MANAGED HARDWARE SERVICES

10.1.1 Compute Hardware

a. The Contractor shall provide compute hardware that meets or exceeds the Hardware Reference Configurations (HRCs) specified in NASA-STD-2805x, and approved in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*.
b. Compute hardware shall meet DRD IT-07, *Vendor Product Performance Specifications*, at the time the order is approved in the ITSM.
c. The contractor may deploy a device that meets the current DRD IT-07 or the previous DRD IT-07 as long as the RITM (order) was approved within 60 days of the latest IT-07 approval of the device type.
d. The Contractor may redeploy compute hardware provided the asset has remaining useful life based on the date of initial deployment and the refresh cycle identified in PWS section 10.1.4.5, Hardware Refresh.
e. The Contractor shall refresh any redeployed compute hardware according to the date of initial deployment.

10.1.2 Included Hardware

The Contractor shall provide with all managed compute hardware:

a. Hardware as required to meet the hardware reference configuration and any other items specified in NASA-STD-2805x that are not offered in PWS section 10.1.3 as optional hardware.
b. For portable systems only, a briefcase or backpack style carrying case, to be selected by customer at time of order, and power adapter.

10.1.3 Optional Hardware

The Contractor shall provide the following hardware as specified per customer request:

a. Performance augmentation: The Contractor shall provide upgrade options to enhance performance of the base system. The Contractor shall provide augmentation options both at the time services are ordered, and for deployed hardware still in use. Augmented systems shall be maintained to the ordered specifications in cases of incidents requiring hardware repair or replacement. Augmentations shall be considered part of the base system and dispositioned with the system in cases of service unsubscription or refresh.
b. External Display Solution: The Contractor shall provide standard and expanded displays that meet NASA-STD-2805x. The Contractor shall provide customers the option to select single or dual displays in any combination of standard or expanded model. The Contractor is responsible for interconnectivity between display(s) and compute hardware. An external display is a stand-alone display, not built in to the compute hardware.
c. Docking Station Solution (portables only): The Contractor shall provide a docking station solution for portable computers that meet NASA-STD-2805x.
d. The Contractor shall provide the following hardware as specified per customer request in accordance with Attachment I-3, Service Level Agreements (SLA), SD-1-A. Optional hardware is available as an augmentation to new and/or previously deployed hardware.

10.1.4 Included Management Services

The Contractor shall perform end-to-end hardware lifecycle management for all managed hardware services.

10.1.4.1 Delivery and Installation

The Contractor shall:

a. Install managed hardware at end-user locations requested for delivery at identified performance sites.
b. Perform installation at the end user's work area to include unboxing, setup, testing for functionality, confirmation of network connectivity, and removal of packaging materials.
c. Deliver managed hardware per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery*and/or in accordance with SLA SD-L-1 for Loaner Services.

10.1.4.2 Delivery to Off-Site Users

The Contractor shall:

a. Provide services for end users stationed at locations other than Centers and Identified Performance Sites by shipping properly configured hardware and software to the end user using drop ship methodology or other NEST COR-approved method.
b. Assume responsibility for all costs associated with shipping and material handling.

10.1.4.3 Reserved

10.1.4.4 Changes

The Contractor shall:

a. Adjust optional services and hardware related to managed hardware per NASA request. Optional hardware specified in PWS section 10.1.3, as well as software services specified in PWS section 10.2 may be added or removed.
b. Complete requests for hardware addition per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery*.
c. Complete requests for hardware removal per Attachment I-3, SLA SD-4, *Completion of Hardware Removal Following Unsubscription or Refresh*.

10.1.4.5 Hardware Refresh

The Contractor shall:

a. Provide a technology refresh plan for refresh of managed hardware per Attachment I-2, DRD IT-04, *Technology Refresh Plan*.
b. Refresh compute hardware per Service Request to update hardware to latest Contractor offerings as proposed and approved in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*
c. Refresh compute hardware at 36 months from the initial deployment date for all configurations with the exception of the PC Standard Desktop and Apple Standard Desktop which shall be refreshed at 48 months from the initial deployment date.
d. Coordinate a date and time for hardware refresh with the end user.
e. Provide hardware refresh with minimum disruption to the end user.
f. Provide and/or replace included hardware and optional hardware as required to maintain compatibility with compute hardware, and compliance with Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*.
g. Document in work log and asset system any items associated with the service that are lost, damaged, destroyed, or stolen for traceability.
h. Provide the ability for customer to request early technology refresh (ETR).

i. Perform individual refresh completions per Attachment I-3, SLA SD-3, *Completion of Refresh Appointment* and SD-4, *Completion of Hardware Removal Following Unsubscription or Refresh*.
j. Retain systems on-site for fourteen (14) calendar days following removal prior to sanitization or disposal to permit recall of data.
k. Sanitize hardware following expiration of retention requirements per Attachment I-3, SLA SM-4.

10.1.4.6 Hardware Restoration

The Contractor shall:

a. Provide restoration of an end user's hardware to full operability when an incident occurs that renders hardware unstable, hardware is lost, damaged, destroyed, inoperable, or exhibits degraded performance. Restoration includes the tasks that are necessary to return managed hardware to an operational state, including correction of hardware faults via repair or replacement, replacement in case of loss or damage, configuration of software load, and restoration or transfer of all user data to replacement hardware.
b. Document in work log and asset system items that are lost, damaged, destroyed, or stolen for traceability.
c. Provide restoration of service per Attachment I-3, SLA IM-1, *Incident Resolution*.
d. Provide a replacement unit of the subscribed hardware reference configuration if the system is rendered unstable or inoperable and the repair time will exceed the applicable restoration SLA.
e. Replace laptop batteries at OEM specified End of Life, or prior in case of failure.
f. Perform backups of systems prior to initiating repair
g. Perform sanitization on media removed from service due to failure, to include physical destruction per Attachment I-3, SLA SM-4.
h. Remove or sanitize storage media prior to shipment of hardware for repair from NASA Centers.

10.1.4.7 Unsubscription

The Contractor shall:

a. Remove services from the end-user environment on request for unsubscription.
b. Document items retrieved, including unique asset identifiers, in the Service Request Work Log.
c. Document in work log and asset system any items associated with the service that are damaged or not present at the time of unsubscription for traceability
d. Complete unsubscription requests, to include hardware retrieval, per Attachment I-3, SLA SD-4, *Completion of Hardware Removal Following Unsubscription or Refresh*.
e. Retain systems on-site for fourteen (14) calendar days following removal prior to sanitization or disposal to permit recall of data.
f. Sanitize hardware following expiration of retention requirements per Attachment I-3, SLA SM-4.

10.1.4.8 Disposal

The Contractor shall sanitize systems prior to shipment from NASA Centers per Attachment I-3, SLA SM-4.

10.1.5 Optional Management Services

The Contractor shall provide the following services for managed hardware as requested:

10.1.5.1 Daily Loaner Device Services

Daily Loaner Device Services is designed to meet end-user short-term requirements for up to 90-calendar days. (Note: If services are required for more than 90-calendar days, the requester should order Compute/Mobile services in lieu of Loaner devices unless it is required for International Travel). Loaner devices listed in the Attachment I-9, CLIN Pricing, specifically L-CLINS, shall be made available for pickup and drop-off at Government-specified sites per Center locations. All loaner devices held longer than 120-calendar days will be automatically converted in ITSM to the applicable service offerings to allow data backup services to be requested by the end-user. All loaner devices shall meet the minimum hardware requirements in accordance with PWS 10.1. Daily Loaner Device Management Services may be added or removed at any time. (WARNING: Loaner devices do not include data backup services and per security requirements are required to be completely sanitized via a full wipe upon return). Daily Loaner Device Services may be added or removed at any time. The contractor shall not utilize Daily Loaner Device Services as a means to provide incident resolution, and NASA utilization of the loaner pool shall not reduce or eliminate the Contractor's responsibility for hardware and software restoration.

The Contractor shall:

a. Provide loaner pick-up/drop-off services at Government-specified sites per Center as locations for end users to pick up and drop off loaner hardware. NASA Centers will provide space allocation required for the loaner pool. If a Center does not have a specified Center location for end-users to pick-up and drop off loaner hardware e.g. Spacebar, the Contractor shall delivery the loaner devices directly to the end-users on-site location or by shipping directly to the end-user for an additional charge for shipping and handling and paid under the CLIN R-99, ODC.
b. Establish a loaner tracking/request/sign-in/sign-out system utilizing NASA's ITSM system. Maintain the status of all services in the loaner pool, and include in these records the beginning and ending dates of each loan and the name of the person to whom hardware was loaned.
c. Charge or exchange batteries to facilitate immediate use.
d. Provide an international power adapter compatible with the loaner hardware on request.
e. Configure Software as subscribed per PWS 10.2-10.2.3, if applicable.
f. Assist customers with set-up and operation of the loaner hardware (e.g., remote access client (e.g., Virtual Private Network (VPN)), as needed.
g. Assist the end user in transfer of data off the loaner as required.
h. Sanitize systems at drop-off via a full wipe, and restore software load as subscribed per PWS 10.2-10.2.3.
i. Prepare returned systems for subsequent pick-up within 8 business hours
j. Complete requests for Daily Loaner Device Services per Attachment I-3, SLA SD-L-1, Completion Time for Delivery of Loaner Services.
k. Safely disinfect all loaner devices using Center for Disease Control (CDC) approved disinfectants prior to re-issuance to any end-users. (https://www.epa.gov/pesticide-registration/list-n-disinfectants-coronavirus-covid-19)

10.2 MANAGED SOFTWARE SERVICES

The Contractor shall provide software management services for both managed hardware services identified in PWS section 10.1, Managed Hardware Services, as well as hardware furnished by NASA or other NASA contractors. To deliver Managed Software Services, the Contractor shall:

a. Package, install, and maintain the operating system, software load as identified in Attachment I-25, *List of Licenses.*
b. Package, install, and maintain additional software as required to deliver NEST-managed services.
c. Configure software per Agency Security Configuration Specifications (ASCS).
d. Provide for security of all software services per PWS section 5.0, Security Management.
e. Propose software configurations per Attachment I-2, DRD IT-13, *Software Load Configuration*.
f. Support software versions one major release preceding current standards as documented in NASA-STD-2804x, by request, to support interoperability with version dependent applications.
g. Deliver managed software as a bundled service when ordered with managed hardware services per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery*.
h. Install requested software to existing deployed hardware per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service.*
i. Restore software services to operable condition when an incident occurs that renders services unstable, inoperable, or with degraded performance. Restoration includes the tasks that are necessary to get an end user's system back to an operational state within the scope of the Contractor's responsibility, including correction of software faults via reconfiguration, reload, and restoration of software and user data.
j. Restore services per Attachment I-3, SLA IM-1, *Incident Resolution*.

10.2.1 Operating System

The Contractor shall:

a. Provide operating systems as specified in NASA-STD-2804x.
b. For physical hardware, install and maintain the requested operating system on the requested physical hardware per NASA-STD-2804x.
c. For virtual machines, install and maintain the requested operating system via virtual machine on the requested hardware. Virtual Machine Operating Systems shall include the following options by hosting operating system:
    - Windows Host with Red Hat Enterprise Linux Guest
    - macOS Host with Windows Guest
    - macOS Host with Red Hat Enterprise Guest
    - Red Hat Enterprise Linux with Windows Guest
d. Configure Operating System to enable Elevated Privileges for user accounts as directed and approved by NASA per Attachment I-3, SLA SD-7.

10.2.2 Software Load

The Contractor shall:

a. Provide software load services per the Software Load Categories specified in Attachment I-25, *List of Licenses*.

b. Package, install, and maintain operating system and software load for core applications for all systems subscribed to software load services.
c. Coordinate with system owner for the installation of software load on Non-NEST provided hardware.
d. The contractor shall provide for end-user requested installation, package, install, and maintain optional software. Optional software titles may not be required by all users, but shall be made available at request at no additional charge.

10.2.3 Software Subscriptions by Title

The Contractor shall:

a. Provide specific applications by title as specified in Attachment I-25, *List of Licenses*. Software Subscription by Title is expected to expand as additional titles are identified for NEST management.
b. Package, install, and maintain software titles as subscribed.

10.2.4 Backup Services

The Contractor shall:

a. Install and configure required clients, and enabling infrastructure required to initiate backup.
b. Complete requests for new backup services to existing hardware per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service*.
c. Notify the customer of backup activation and provide required instructions to the end-user for operating the backup service to protect NASA data.
d. Provide remediation of failed backups to mitigate data loss incidents.
e. Remediate instances where subscribed backups are not being performed via customer engagement.

10.3 UNMANAGED HARDWARE ACCESSORIES

The Contractor shall:

a. Propose compute accessories to complement managed hardware in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*, to be approved by the EUSO.
b. Offer only items that are compatible with and suitable for use with contractor provided managed hardware.
c. Make products available for purchase in the ITSM system.
d. Ensure products offered are cleared for NASA use per Supply Chain Management Requirements.
e. Provide products with manufacturer's warranty.
f. Provide proof of order with products.
g. Deliver products directly to the end user.
h. Provide and support hardware drivers as required.
i. Provide end-user consultation for placing orders.
j. Accept returns directly from the customer and facilitate return to the vendor if return is requested within 30 days.
k. Credit returned items or remove them from invoicing.

Accessories provided via this method shall be titled to the Government and will be unmanaged by the Contractor following delivery. Government approval of proposed products may be limited as required to ensure enforcement of NASA policies, such as requirements for management of

Government Property. Products anticipated to be offered as unmanaged systems include, but are not limited to, adaptive hardware, input devices, and encrypted USB storage devices. Internal upgrade components shall only be offered as managed services per PWS section 10.1.3, Optional Hardware. Accessories purchased will not be returned to the contractor following unsubscription of managed hardware services.

10.4 RESERVED

10.5 SERVICE TESTING

The Contractor shall:

a. Provide access to test hardware at all Centers that permit customer testing of all managed hardware and managed software services currently deployed. Testing offerings shall be suitable for verifying compliance to NASA requirements, and compatibility testing with other software and components.
b. Provide an Agency total of 30 fully licensed virtual disk images, compliant with NASA-STD-2804 virtualization clients, that represent the functional software builds as proposed in Attachment I-2, DRD IT-13, *Software Load Configuration*.

10.6 ONE-TIME SERVICES

10.6.1 Software Wipe and Reload

The Contractor shall:

a. Perform data backup, sanitize systems, and restore software configuration to original baseline.
b. Coordinate a time with the end user to perform the sanitization and reconfiguration as required.
c. Perform software wipe and reload per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service*.

10.6.2 Data Transfer

The Contractor shall provide, at NASA request, transfer of end-user data from:

a. NEST-managed hardware to NEST-managed hardware
b. Non-NEST-managed hardware to a NEST-managed hardware
c. NEST-managed hardware to a non-NEST-managed hardware

10.6.3 Sanitization

The Contractor shall sanitize Government hardware to support disposal of non-Contractor managed assets.

10.6.4 Non-standard Hardware Installation

The Contractor shall:

a. Provide peripheral installation as requested by NASA to include hardware drivers and other management software.
b. Test hardware for proper operation and address compatibility issues introduced via removal if hardware or drivers conflict with operation of NEST-provided services.

10.6.5 Moves

The Contractor shall:

a. Relocate managed hardware and connected peripherals on request to include deinstallation, material handling, and reinstallation of managed hardware, optional hardware, included hardware, and any connected peripherals. Moves may be internal to Center, or between Centers.

b. Assume responsibility for safe transit of hardware including material handling, shipping, and associate costs.
c. Coordinate with Center move coordinator(s) and other supporting contractors for the scheduling and execution of hardware moves.

11.0 MOBILE SERVICES

NASA's vision is to enable the work force to be flexible in its ability to work from anywhere. To deliver mobile services according to this philosophy, the Contractor shall:

a. Provide managed mobile device services in a subscription model in response to NASA requests for services submitted and approved via NASA's ITSM system.
b. Remove services unsubscribed by NASA at no additional cost as requirements change.
c. Modify services as requested for elements specified as optional services.
d. Provide mobile hardware per minimum specifications as defined in the NASA-STD-2805x, *Minimum Hardware Configurations*.
e. The Contractor shall propose mobile device offerings per Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications.*
f. Deliver mobile services per Attachment I-3, SLA SD-1, *Completion of Hardware Installation & Delivery*.
g. Perform changes to existing services per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service*.

11.1 CELLULAR SERVICES

The Contractor shall provide cellular devices, as defined in PWS section 11.2 Cellular Phone Device and PWS section 11.3 Smartphone Device (such as Androids and iPhones), as specified by individual HRCs in the NASA Hardware Standards, currently NASA-STD-2805x, *Minimum Hardware Configurations*.

a. The Contractor shall maintain the current cellular numbers assigned to existing cellular devices.
b. The Contractor shall provide unlimited voice, data, and text messaging services for all cellular devices with no roaming or long-distance charges.
c. The Contractor shall provide an end-user configurable hot spot from all service offering carriers on all Smartphone Device options, with unlimited data.

11.2 CELLULAR PHONE DEVICE

a. The Contractor shall provide a cellular phone device and unlimited basic cellular services including voice and messaging with unlimited data plans including push-to-talk.
b. The Contractor shall provide a cellular phone device that includes the following consumable accessories: wall charger, car charger, hands-free headset, and the customer's option of either a carrying case (holster) or slim case.

11.3 SMARTPHONE DEVICE

The Contractor shall:

a. Provide smartphone devices that run a mobile operating system that can make and receive phone calls over a cellular network (e.g. iOS and Android mobile).
b. Offer a smartphone device that includes the following consumable accessories: computer synchronization cable where necessary, wall charger, car charger, a hands-free headset, and the customer's option of either a carrying case (holster) or slim case.
c. Provide the applicable application software (if not native on the device) to enable the viewing of word processing, spreadsheets, presentation, and Portable Document Format (PDF) data files on such devices as defined in the latest NASA Standard, currently NASA-STD-2804x, *Minimum Interoperability Software Suite*.
d. Ensure that any smartphone device deployed to the end users is compliant with NASA IT Security Requirements, as defined in NASA IT Security policy NPR 2810.1x, *Security of Information Technology* and applicable NASA IT Security handbooks, and is compatible with the NASA Mobile Device Management (MDM) solution.
e. Provide printing capabilities to Agency printing resources from mobile devices.

11.4 TABLET DEVICE

The Contractor shall:

a. Provide tablets that run a mobile operating system, (e.g., iOS, Android, Windows) and provide email, light office automation, web browsing capabilities, and access to web applications in a touch-enabled, highly portable, lightweight form factor, in accordance with the individual tablet HRCs in the current NASA-STD-2805x, *Minimum Hardware Configurations* and NASA-STD-2804x, *Minimum Interoperability Software Suite*.
b. Offer a tablet device that includes the following consumable accessories: wall charger with cable, computer synchronization cable where necessary, and protective case.
c. Ensure that any tablet device deployed to the end user is enrolled in the NASA MDM solution. All functionality of such a device shall be governed by the server-based policies as defined by NASA's messaging service and a corresponding MDM solution that supports device-level policy enforcement and device-level data encryption. The Contractor shall ensure the tablet devices are configured, managed, and supported with NASA's MDM solution.
d. Provide the appropriate software that supports synchronization between the tablet device and the associated end user's computing device.
e. Maintain the device's compatibility with Agency desktop/laptop systems/software as it relates to the synchronization and transfer of data.
f. Provide (if not native on the device) the applicable application software to enable the viewing of word processing, spreadsheets, presentation, and PDF data files on such devices as defined in the latest NASA standards, currently NASA-STD-2804x, *Minimum Interoperability Software Suite.*
g. Provide an end-user configurable hot spot from all service offering carriers on all Tablet Device options, with unlimited data.

11.5 PAGER DEVICE

The Contractor shall:

a. Provide pager devices and services, primarily used by essential services personnel, to receive and, in some cases, transmit alert signals and/or short messages.

b. Provide a standard pager device with the following accessories: belt clip and any end-user documentation necessary.
c. Provide the required plan-based communication service for use anywhere in the CONUS with no roaming or long-distance charges. The Contractor shall provide plans that include a base number of messages included per month for the pager device as well as unlimited messages.
d. Provide message to notification and voicemail notification services.
e. Provide the services required for the pager to receive notification from a voicemail system.
f. Provide the end user with the capability to set up a telephone number where they are notified of messages received and can specify a time range to receive the notification.

11.6 MOBILE HOTSPOT DEVICE (MIFI)

The Contractor shall:

a. Provide hot spot devices and services that provide a wireless connectivity device that offers cellular access by multiple end-user systems.
b. Offer the devices from all service offering carriers and offer unlimited hot spot data plans per carrier.
c. Offer an international service option.

11.7 INTERNATIONAL MOBILITY SERVICES

a. The Contractor shall provide an unlimited international plan for voice, data, and text communications outside of the United States for cellular mobile devices that includes the capability to make and receive calls to and from the United Status and to and from foreign countries.
b. The Contractor shall provide an unlimited international plan for data and text communications outside of the United States for tablet and hot spot mobile devices with data service options.
c. International mobility services are orderable for NEST and Government owned mobile devices subscribed to NEST services.

11.8 DATA PLANS SERVICE FOR OTHER MOBILE TABLET DEVICES (GOVERNMENT-OWNED)

a. The Contractor shall provide unlimited data plan services for other mobile tablet devices (not listed in previous Mobile sections) that provide data connectivity for Government-owned equipment. The Contractor is not responsible for the Government-owned device. The Contractor only provides the data plans for devices that are compatible with the carriers' service capabilities.
b. The Contractor shall provide domestic data plans for anywhere in the CONUS with unlimited data and no roaming. The plan shall offer multiple hot spot data plans from all service offering carriers.
c. The Contractor shall provide an option for international data. The user is required to subscribe to a domestic plan to add an international plan. The service shall be billed for a minimum of one (1) month.

11.9 MOBILE DEVICE MANAGEMENT

a. The Contractor shall ensure that all Contractor-provided mobile devices with an MDM-capable mobile operating system such as, but not limited to, iOS and Android, shall be enrolled in the Agency's MDM solution (currently MaaS 360) as defined in PWS section

9.0, Infrastructure Operations. Enrollment includes registration of the device in the MDM service, as well as installation of all applicable applications locally installed on the mobile device to ensure appropriate integration with the MDM solution.

b. The Contractor shall also provide a capability to enroll mobile devices that are not provided by the Contractor such as capable Government owned (GFE) devices, capable personally owned devices, or capable business-owned devices, but shall not license or enroll those devices until requested by NASA to include those devices.

11.10 MOBILE DEVICE REFRESH AND DEPLOYMENT

The Contractor shall deliver and refresh mobile device hardware to include cellular phones, smartphones, and tablets. Refresh for mobile devices shall be at 24 months from the initial date of deployment. Redeployment of a device does not reset the initial deployment date. The Contractor shall:

a. Provide a technology refresh plan for refresh of managed mobile hardware per Attachment I-2, DRD IT-04, *Technology Refresh Plan*.
b. Provide a storefront capability for deployment of devices where the Center has requested the storefront delivery method.
c. Provide for scheduled technology refresh of cellular device hardware and required peripherals as well as initial delivery of application software.
d. Ensure that end users are able to keep existing phone numbers when refreshing cellular devices.
e. Complete mobile refreshes per Attachment I-3, SLA SD-3, *Completion of Refresh Appointment.*
f. Integrate new device and refresh orders for devices that have reached the user's refresh date using NASA's ITSM system for requesting, approving, deferring, and/or unsubscribing devices.
g. Consider devices found to be defective during refresh as a warranty item and replace as part of the regular device maintenance option.
h. Provide the ability for end user to request early technology refresh (ETR).

11.11 MACHINE-TO-MACHINE WIRELESS SERVICE

The Contractor shall:

a. Provide a domestic machine-to-machine (M2M) wireless service that will enable NASA to obtain carrier data communications with potentially a variety of connected devices. Examples of M2M wireless uses at NASA include air/water/soil monitoring devices, interactive billboards, connected thermostats in buildings for real-time adjustments, fleet tracking devices, remote video surveillance cameras, defibrillator data tracking, asset tracking, remote monitoring, physical plan monitoring, sensors, etc. No hardware or hardware maintenance will be required of the Contractor as a part of this service.
b. Provide a monthly service that will be based upon the plan and data volume. NASA will be responsible for limiting any overages. The Contractor shall invoice any overage charges as incurred.
c. Provide data option service levels, to include handling limit overages.

11.12 MOBILITY SERVICES REPORTING

The Contractor shall:

a. Provide all mobile device service data in a secure, online, searchable database with access controls defined by the EUSO, in accordance with Attachment I-2, DRD IT-01, *Agency Mobile Services Detail Reports*.
b. Make available monthly a summary report related to mobile services, in accordance with Attachment I-2, DRD IT-01, *Agency Mobile Services Detail Reports*, showing domestic usage of all services for all mobile device services.
c. Provide a detailed report showing international usage to include voice, data, and text with all itemized charges for all mobile devices subscribed to international service in accordance with Attachment I-2, DRD IT-01, *Agency Mobile Services Detail Reports*.

11.13 MOBILE SERVICE RESTORATION

The Contractor shall:

a. Provide restoration of an end user's device to full operability when an incident occurs that renders the device unstable, inoperable, or with degraded performance. Restoration includes the tasks that are necessary to return the mobile device services back to an operational state, including correction of hardware faults via repair or replacement, replacement in case of loss or damage, configuration of software load, and assistance with the restoration and transfer of all user data to replacement device.
b. Provide restoration of service per Attachment I-3, SLA IM-1, *Incident Resolution*.
c. Provide a replacement device if the end user's device is rendered unstable or inoperable and the repair time will exceed the applicable restoration SLA.
d. Perform sanitization on media removed from service due to failure, to include physical destruction per Attachment I-3, SLA SM-4.
e. Remove or sanitize storage media prior to shipment of equipment for repair from NASA Centers per Attachment I-3, SLA SM-4.

11.14 MOBILE LOANER POOL

Mobile Devices subscribed to Loaner Pool Management are made available for pickup and drop-off from the NEST contractor to meet end-user needs for temporary use. Mobile Devices as defined in PWS 11.1-11.6 will be assigned for Loaner Pool Management via service request by the subscribing organization. Loaner Pool Management services may be added or removed at any time. The contractor shall not utilize loaner pool devices as a means to provide incident resolution, and NASA utilization of the loaner pool shall not reduce or eliminate the Contractor's responsibility for hardware and software restoration.

The Contractor shall:

a. Provide loaner pick-up/drop-off services at Government-specified sites per Center as locations for end users to pick up and drop off loaner devices. NASA Centers will provide space allocation required for the loaner pool.
b. Establish a loaner pool tracking/request/sign-in/sign-out system utilizing NASA's ITSM system. Maintain the status of all services in the loaner pool, and include in these records the beginning and ending dates of each loan and the name of the person to whom each device was loaned.
c. Provide all accessories for the loaner device per PWS 11.2-11.6.
d. Charge or exchange batteries to facilitate immediate use.
e. Provide an international power adapter compatible with the loaner device on request.

f. The Center shall have the option to designate which Center organizational unit(s) will have access to the system.
g. When a loaner device is returned by the end user, sanitize via factory reset and restore to baseline configuration.
h. Prepare returned systems for subsequent checkout within 8 business hours.
i. Complete requests for Mobile Loaner Pool per Attachment I-3, SLA SD-L-1, Completion Time for Delivery of Loaner Service.

11.15 DELIVERY TO OFF-SITE USERS

The Contractor shall:

a. Provide services for end users stationed at locations other than Centers and Identified Performance Sites by shipping properly configured hardware and software to the end user using drop ship methodology or other NEST COR-approved method.
b. Assume responsibility for all costs associated with shipping and material handling.
c. Complete requests for Delivery to Off-Site Users per Attachment I-3, SLA SD-L-1, Completion Time for Delivery of Loaner Service.

11.16 UNMANAGED HARDWARE ACCESSORIES

The Contractor shall:

a. Propose mobile accessories to complement managed devices in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*, to be approved by the EUSO.
b. Offer only items that are compatible with and suitable for use with contractor provided managed devices.
c. Offer all Government-approved accessory options for mobile devices in the NASA ITSM ordering system.
d. Ensure products offered are cleared for NASA use per Supply Chain Management Requirements as cited in PWS section 5.1.4 (l), *System Vulnerability Management and Configuration*.
e. Provide products with manufacturer's warranty.
f. Provide proof of order with products.
g. Deliver products directly to the end user.
h. Provide end-user consultation for placing orders.
i. Accept returns directly from the customer and facilitate return to the vendor if return is requested within 30 days.
j. Credit returned items or remove them from invoicing.

Accessories provided via this method shall be titled to the Government and will be unmanaged by the Contractor following delivery. Government approval of proposed products may be limited as required to ensure enforcement of NASA policies. Accessories purchased will not be returned to the Contractor following unsubscription of managed device services.

12.0 PRINT SERVICES

In support of NASA's missions and end users, the Government requires flexibility in the provisioning and management of print services. To provide this flexibility, NASA requires managed hardware and managed services to be available separately. These services are hereafter referred to as print services. Print services shall include digital multifunction printing devices (MFDs) and printers. NASA anticipates that most users will subscribe to a bundle of services to meet the needs of the end user. The NEST Print Services Subscription Service Model is represented in Table 12.0-1.

Table 12.0-1. NEST Print Services Subscription Service Model.

Managed Hardware	Print Device	Hardware reference configuration per Addendum 1 to Attachment I-1, *Minimum Print Hardware Requirements*
	Optional Equipment	Equipment and accessories specified at time of service order or via changes though the life of the service
	Included Management Services	Requirements that apply to all managed hardware services
	Optional Management Services	Optional service specified at time of service order or via changes thoughout the life of the service

To deliver services within the NEST print subscriptions the Contractor shall:

a. Provide managed print device services in a subscription model in response to NASA requests for services submitted and approved via NASA's ITSM system.
b. Provide managed hardware services, managed finishing solutions, or combinations of both to meet NASA end-user requirements.
c. Remove services unsubscribed by NASA at no additional cost as requirements change.
d. Modify services as requested for elements specified as optional services.
e. Manage print services hardware per minimum specifications as defined in Addendum 1 to Attachment I-1, *Minimum Print Hardware Requirements*, and approved in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*.

12.1 GENERAL PRINT SERVICES

The Contractor shall provide a detailed and thorough technical approach for ordering, delivering, maintaining, refreshing, and unsubscribing all print solution services using NASA's ITSM system. The Contractor shall:

a. Provide all print service requirements in accordance with NASA's requirements in Addendum 1 to Attachment I-1, *Minimum Print Hardware Requirements*.
    i. The pricing model for print services shall include the total price to deliver the service under each model to include all maintenance, support, and/or replacement costs.
b. Provide an option for cost per copy for all print services.
c. Provide an option for volume banding for all print services.
    i. Monthly volume band impressions for black and white shall fall into the following maximum quantities:
        (a) 1,250
        (b) 2,500
        (c) 5,000
        (d) 10,000
    ii. Monthly volume band impressions for color shall fall into the following maximum quantities:
        (a) 1,250
        (b) 2,500
        (c) 5,000
        (d) 10,000
    iii. The Contractor shall report, on a monthly basis, black and white and/or color print impressions in excess of the total Agency volume bands ordered through the NASA

ITSM System. The Contract shall invoice the Government for the print impressions that exceed the total Agency monthly volume bands at the price per copy for black and white or color prices in Attachment I-9, *CLIN Pricing*.

12.2 PRINT DEVICES

The Contractor shall provide print devices meeting or exceeding the Hardware Reference Configurations (HRCs) specified in Addendum 1 to Attachment I-1, *Minimum Print Hardware Requirements*, and approved in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*. Current HRCs include:

- B&W Printer
- Color Printer
- B&W MFD
- B&W MFD (Current minimum of 35 ppm) with Finisher
- Color MFD
- Color MFD (Current minimum of 35 ppm) with Finisher
- Color MFD (Current minimum of 55 ppm) with Finisher and Fiery 3
- Legacy CLIN J-1A B&W Printers
- Legacy CLIN J-2A Color Printers
- Legacy CLIN K-1A B&W MFD 35 ppm
- Legacy CLIN L-1A B&W MFD 35 ppm with finisher
- Legacy CLIN L-2 B&W MFD 45 ppm with finisher
- Legacy CLIN L-2A B&W MFD 45 ppm with finisher
- Legacy CLIN L3 B&W MFD 55 ppm with finisher
- Legacy CLIN L-3A B&W MFD 55 ppm with finisher
- Legacy CLIN M-1A Color MFD 35 ppm
- Legacy CLIN N-1A Color MFD 35 ppm with finisher
- Legacy CLIN N-2 Color MFD 45 ppm with finisher
- Legacy CLIN N-2A Color MFD 45 ppm with finisher
- Legacy CLIN N-3A Color MFD 55 ppm with finisher

The Contractor shall deploy only devices that have remaining useful life per PWS section 12.6.4, Hardware Refresh. Redeployment of previously issued devices is permissible given the specifications are in compliance with Addendum 1 to Attachment I-1, *Minimum Print Hardware Requirements* and Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications* at the date of initial deployment.

12.3 PRINT SERVICES REQUIREMENTS

For all print devices, the Contractor shall provide the following print services:

a. Management for all print queues
b. Capability to print on recycled paper and/or on lighter paper (e.g., 64g/m2)
c. Active Directory Integration and Authentication
d. Automated Print Driver Installation
e. Network Connectivity
f. Configure duplex printing as the “default” print setting to reduce consumption of natural resources and cost.

g. Configure black and white printing on all NEST color print devices as the “default” print setting to reduce consumption of natural resources and cost.

12.3.1 MFD Print Services Requirements

For all MFD print devices, the Contractor shall provide the capabilities in PWS section 12.3, Print Services Requirements, and the following capabilities:

a. Secure Printing and Encryption with FIPS 201 Smartcard (PIV card) Capability initiated by the end user, and then released from the selected MFD via PIV card authentication
b. Copy
c. Scanning to email and file
d. Facsimile
e. N-Up printing capability (printing multiple pages on one sheet of paper)

12.4 FINISHING SOLUTIONS

The Contractor shall provide the following print service finishing solutions:

a. Finisher with the following capabilities:
   i. Output offset
   ii. Output collating (sort)
   iii. Output stack
   iv. Output stapling
b. Automatic hole punching

12.5 PRINT SERVICES CONSUMABLES

The Contractor shall provide all print service consumables (e.g. toner, staples, other replenishable items, and repair parts) including the disposal of consumables. The Contractor shall:

a. Provide, install, manage, and replace all consumables and replacement parts for print devices.
b. Remove and dispose of all toner and all equipment parts in accordance with Federal and NASA requirements in accordance with Attachment I-2, DRD IT-02, *Toner and Waste Disposal Plan*.

12.6 PRINT DEVICE MANAGEMENT SERVICES

The Contractor shall perform end-to-end device lifecycle management for managed print service devices including adherence to applicable IT Security requirements per PWS section 5.0, as well as entering and updating print device asset information into the SACM system as cited in PWS section 6.6.

12.6.1 Delivery and Installation

The Contractor shall:

a. Install managed devices at end-user locations requested for delivery at identified performance sites, to include unboxing, setup, testing for functionality, confirmation of network connectivity, and removal of packaging materials.
b. Deliver managed devices per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery*.

12.6.2 Moves

The Contractor shall:

a. Relocate managed print devices on request to include deinstallation, moving, shipping, and reinstallation. The Contractor is responsible for safe transit of devices including all costs for shipping and material handling.
b. Coordinate with Center move coordinator(s) and other supporting contractors for the scheduling and execution of device moves.

12.6.3 Changes

The Contractor shall:

a. Adjust finishing solutions and equipment related to managed hardware per NASA request. Optional equipment specified in PWS section 12.4, as well as services specified in 12.7 may be added or removed.
b. Complete requests for hardware addition per Attachment I-3, SLA SD-1, *Completion of Hardware Installation and Delivery*.
c. Complete requests for hardware removal per Attachment I-3, SLA SD-4, *Completion of Hardware Removal Following Unsubscription or Refresh*.
d. Complete all changes not otherwise specified per Attachment I-3, SLA SD-2, *Completion of Software Installation or Change to Existing Service*.

12.6.4 Hardware Refresh

The Contractor shall:

a. Refresh print device hardware per Service Request to update devices to latest contractor offerings as proposed and approved in Attachment I-2, DRD IT-07, *Vendor Product Performance Specifications*.
b. Refresh managed print hardware devices sixty (60) months from the initial date of deployment.
c. Provide a technology refresh plan for refresh of managed hardware per Attachment I-2, DRD IT-04, *Technology Refresh Plan*.
d. Provide for customer to request Early Technology Refresh (ETR).
e. Complete print refreshes per Attachment I-3, SLA SD-3-P, *Completion of Refresh Appointment*.

12.6.5 Hardware Restoration

The Contractor shall:

a. Provide restoration of an end user's device to full operability when an incident occurs that renders hardware unstable, equipment is lost, damaged, destroyed, inoperable, or exhibits degraded performance. Restoration includes the tasks that are necessary to return managed hardware to an operational state, including correction of hardware faults via repair or replacement, replacement in case of loss or damage, configuration of software load, and restoration or transfer of all user data to replacement device.
b. Document items that are lost, damaged, destroyed, or stolen in work log and asset system for traceability.
c. Provide restoration of service per Attachment I-3, SLA IM-1, *Incident Resolution*.
d. Provide a replacement unit of the subscribed hardware reference configuration if the system is rendered unstable or inoperable and the repair time will exceed the applicable restoration SLA.
e. Perform sanitization on media removed from service due to failure, to include physical destruction per Attachment I-3, SLA SD-4, *Completion of Hardware Removal Following Unsubscription or Refresh*.

f. Remove or sanitize storage media prior to shipment of equipment for repair from NASA Centers.

12.6.6 Unsubscription

The Contractor shall:

a. Remove services from the end-user environment on receipt of request for unsubscription.
b. Document items retrieved, including unique asset identifiers, in the Service Request Work Log.
c. Sanitize equipment prior to following expiration of retention requirements.
d. Complete unsubscription requests, to include hardware retrieval, per Attachment I-3, SLA SD-4, *Completion of Hardware Removal Following Unsubscription or Refresh*.

12.6.7 Disposal

The Contractor shall sanitize systems prior to shipment from NASA Centers per Attachment I-3, SLA SM-4.

12.7 REPORTING REQUIREMENTS FOR ALL PRINT SERVICES

The Contractor shall provide impression utilization reporting for all subscribed print service devices. The reporting shall include beginning and ending meter counts, total impressions per month, and a cumulative number of annual impressions per device. The Contractor shall:

a. Assume responsibility for taking accurate automated impression utilization counts for near real-time reporting for all networked print services.
    i. Non-networked print services reporting shall consist of monthly impression counts for each print service delivered.
    ii. Impression counts shall be taken for scan, fax, copy, and print functions for all print services in accordance with Attachment I-2, DRD IT-08, *Agency Print Services Detail Report*.
b. Implement a near real-time report capability that will allow the Government to view number of impressions (black/white, color) for print services. This capability shall include a dashboard that allows the Government to view print services data by device (asset number), Center, location, user, organization, date range, price model, or service category.
c. Make available a detailed report showing individual usage of all services for all printer devices in accordance with Attachment I-2, DRD IT-08, *Agency Print Services Detail Report*.
d. Capture the initial meter reading for each NEST print device when a print service is ordered from that device, as a basis for reporting and validating of print utilization.

12.8 PRINT VOLUME UTILIZATION AND USAGE ANALYSIS SERVICES

The Contractor shall:

a. Provide print volume utilization and usage analysis services for the subscribed print services.
b. Review, on an annual basis, the total Agency print utilization requirements by Center and make recommendations to delete and/or reallocate print resources to help reduce the Government's overall print service cost.
c. Continually monitor print utilization at each Center using NASA's ITSM system and/or other analytical tools, and submit to the Government the results of the analysis of statistical usage data by service type, and present a business case supporting any recommendations in accordance with Attachment I-2, DRD IT-08, *Agency Print Services Detail Report*.

12.9 ENERGY CONSERVATION

NASA is committed to taking an active role in limiting its environmental impact and promoting superior energy efficiency by aligning with the Environmental Protection Agency's (EPA's) ENERGY STAR initiative. In accordance with this commitment, the Contractor shall:

a. Comply with Imaging Equipment Key Product Criteria (effective January 1, 2014) set forth in ENERGY STAR, which shall include "low-power mode."
b. Only provide items that comply with and meet the U.S. EPA Comprehensive Procurement Guidelines (recycled content) or the U.S. Department of Agriculture BioPreferred (biobased) programs.

12.10 PRINT SERVICES AND CONSUMABLES FOR GOVERNMENT-OWNED EQUIPMENT

The Contractor shall provide restoration and consumables for Government-owned equipment that is subscribed for these services. The Government shall be able to subscribe or unsubscribe Government-owned equipment where this service is required. The Contractor shall provide a fixed price offering per unit for the B&W and Color Government-owned equipment that is subscribed for this service.

a. The Contractor shall provide restoration for a subscribed Government-owned print device to full operability when an incident occurs that renders hardware unstable, inoperable, or with degraded performance. Restoration includes the tasks that are necessary to get a print device back to an operational state within the scope of the Contractor's responsibility including correction of hardware faults via repair, and restoration of configuration issues.
b. All consumables shall be included for the government owned equipment when this service is requested.
c. No refresh is required for Government-owned print devices.

12.11 LEGACY PRINT DEVICE SUPPORT

The Contractor shall provide support for legacy print devices, as defined in Attachment I-24, *Glossary of Terms,* which are in the NEST end-user environment. Legacy print devices shall not be available for order as a new service (PWS section 12.6.1), nor will they be available as a choice for refresh (PWS section 12.6.4). For legacy print devices, the Contractor shall:

a. Provide all print services requirements listed in PWS section 12.3.
b. Provide all print service consumables listed in PWS section 12.5.
c. Provide the all print device management services as listed in PWS section 12.6.

13.0 ENHANCED SUPPORT SERVICES

Enhanced Support Services are intended as an augmentation to the standard system administration services provided under the NEST Contract as well as a vehicle for the Government to acquire computer support for other functionality. For periods greater than one (1) month, the Government will provide office space, in close proximity to the end users being served, for the individual performing the Enhanced Support Services. The Contractor shall provide Enhanced Support Services for the following labor categories:

- System Administrator 1 through 4
- Subject Matter Expert 1 through 4
- Computer Operator I through V
- Peripheral Equipment Operator

- Personal Computer Support Technician
- System Support Specialist
- Systems Engineer 1 through 4

The Contractor shall provide firm fixed price level of effort other direct costs (ODC) to support Enhances Support Services for PWS sections 1-13. ODC's are costs not previously identified as a direct material cost, direct labor cost, or indirect cost and can be identified specifically with a final cost object.

ODCs can include costs such as but not limited to vehicle rental, travel, special tooling and/or equipment.

Prior to the Government ordering any Enhanced Support Services or ODC, the Center Relationship Manager (CRM), requiring organization, and NEST Contractor will meet to discuss the requirement and determine the appropriate labor category or categories and ODCs necessary to fulfill the requirement.

Enhanced Support Services shall be available for order via NASA's ITSM system, on either a daily or monthly basis. The Government will identify the number of days for all orders requiring daily services. Enhanced Support Services are for staff augmentation for Center or Program requirements above and beyond what is required to support the NEST Contract requirements as delineated in PWS Sections 1-12.