ATTACHMENT I-24
GLOSSARY OF TERMS

_________ x – The “x,” as used in the RFP after the designator for a policy, procedural requirement, or standard, refers to the fact that the latest signed version of the policy, procedural requirement, or standard approved for use by NASA is the Contract requirement at any given point in time. The relevant Contract requirements will change accordingly. The latest signed version of these documents should be used by the offerors for proposal preparation, and pricing should account for these changing requirements.

Acquisition Cost – The cost to acquire a tangible capital asset including the purchase price of the asset and costs necessary to prepare the asset for use. Costs necessary to prepare the asset for use include the cost of placing the asset in location and bringing the asset to a condition necessary for normal or expected use.

Active Directory – Active Directory provides a single source to locate any object within an organization's network. The global catalog is a service within Windows Server that allows users to find any objects to which they have been granted access.

Asset Management – An accounting process for monitoring hardware and software provided under the Contract. Records include but are not limited to the purchase price, depreciation, business unit, and location.

Authentication – A security process designed to establish the validity of a transmission, message, or originator or to verify an individual’s eligibility to receive specific categories of information.

Authorization – The process of granting or denying access to system objects based on an individual or entity’s identities, roles, or other qualifying characteristics (e.g., clearance level).

Availability period – The amount of time the system(s), or the total system, is functioning so that the end user can access the resources provided by that system.

Availability – Ability of a component or service to perform its required function at a stated instant or over a period of time. It is usually expressed as the availability ratio, i.e., the proportion of time that the service is actually available for use by the end users within the agreed upon service hours.

Business Hours – 6 am to 6 pm local time at the site of performance.

Cellular Device – A pocket-sized computing device, having a display screen with touch or push-button input and miniature keyboard with voice and data capabilities.

Center Technical Monitor – Will be designated at each Center by the ATODO to oversee technical performance in accordance with the NEST Contract.

Close of Business (COB) – 6:00 pm local time at the installation where the service is to be provided.

Cloud computing – Internet- (“cloud-”) based development and use of computer technology (“computing”). It is a paradigm shift whereby details are abstracted from the users who no longer
need knowledge of, expertise in, or control over the technology infrastructure “in the cloud” that supports them. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on the Internet, and it typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.

**Collaboration (synchronous)** – Synchronous collaboration capabilities enable a same time, different place interaction between collaborators. Synchronous communications occur in real time and can take place face-to-face, and as technology has evolved, can take place irrespective of distance (e.g. video conferences, telephone conversations and instant messaging).

**Computing Device Configuration** – The hardware and software characteristics associated with a computing device. Hardware characteristics include: CPU, RAM, disk storage, size of monitor, specialty cards (e.g., wireless network card and video card) installed in the system unit, and devices attached directly to the system unit. Software characteristics include: identification of commercial-off-the-shelf (COTS) software in use on the workstation, the operating system, and a description of any commonly distributed custom applications.

**Computing Device** – Distributed computing resource, either networked or standalone, consisting of a CPU, keyboard, monitor, and a screen manipulation device, such as a mouse. This typically includes Windows-, Apple-, Linux-, and UNIX-based workstations. This definition excludes mainframes and supercomputers.

**Confidentiality** – Assurance that information is not disclosed to unauthorized entities or processes.

**Configuration Item (CI)** – Any uniquely identifiable component or other service asset that is managed in order to deliver an IT service.

**Configuration Management Database (CMDB)** – A database used to store Configuration Items (CI) throughout their lifecycle. The Configuration Management System (CMS) maintains one or more CMDBs and each database stores attributes of CIs, and relationships with other CIs.

**Consumables** – Product parts or supplies (except paper) that are consumed during the operation of the product, require replacement based on usage, and are necessary to provide the functionality of the device. Consumables include but are not limited to the following: single and full-color toner cartridges, toner developer, dry ink, dry imager, fuser oil and fusing rollers, cleaning blades, pickoff fingers, photoconductors, photoreceptor belts and drums, staples wire, binder material, and binder adhesive for both black and white and color hardware.

**Consumer product line** – The product line that is identified by the hardware vendor as intended for business use and not intended for home use.

**Core Software** – Software included for all systems subscribed to Software Load services.

**Critical Uplift** – The escalation of Return to Service to its highest (most stringent) value in terms of performance and service characteristics. The set of services affected in this manner includes Hardware Maintenance and System and Applications Software maintenance.

**Customer Relationship Management (CRM)** – A strategy or philosophy designed to optimize end-user and customer benefits, value, and satisfaction. It is a widely adopted system that helps
organizations implement end-user-centric actions, respond better to complaints or feedback, develop end-to-end processes, and optimize end-user support. CRM involves applying policies, processes, and technologies to ensure that current end users and customers are retained and satisfied and new end users and customers are gained.

**Customer Satisfaction** – The measure of how products and services supplied by the Contractor meet or surpass customer expectation. It is seen as a key performance indicator within business.

**Data-at-Rest (DAR)** – All data in computer storage (excluding data traversing a network or temporarily residing in computer memory). DAR can be archival or reference files that are changed rarely or never. DAR can also be data that is subject to regular but not constant change.

**Device-Agnostic** – The capacity of a computing component to work with various systems without requiring any special adaptations. In the context of the NEST contract, the ability for a desktop, laptop, tablet, or smart phone to work with NASA systems and applications and have the content be properly displayed and functional.

**Discretionary** – The power or right to make official decisions using reason and judgment to choose from among acceptable alternatives.

**Downtime** – The amount of time when an end user’s access to the Contractor’s services is impaired. Downtime for each Incident is defined as the period between the time of failure and the time that the system is returned to the end user fully operational.

**Early Tech Refresh (ETR)** – The replacement of a seat before its scheduled refresh date.

**eBanking** – A type of secure access in which the end user is not physically or logically attached to the internal data network. The end user must enter their identity and credentials to gain access, and the application then controls what transactions and functions they can perform dependent on their level of authorization and digital rights assigned to them. The data is served and stays on the internal servers, not the end-user device. The only requirement of the end user is an updated secure browser as all the data and transactions execute on the secure internal server. This type of secure access is widely deployed in industry and NASA is interested in using a similar implementation to secure its transactions and data.

**Elevated Privilege** – Elevated privileges are any access rights or permissions that allow the user that holds them to access system control, monitoring, or administration functions. This includes functions such as installing, upgrading, or significantly changing or patching software, including the computer’s operating system.

**End-users affected** – The calculation of the number of end users impaired by an outage. No end user shall be counted more than once per downtime event even if more than one of their NEST services is not available. If the number of end users impaired cannot be measured with certainty, the Contractor shall estimate the number of end users impaired using the following rules based on the best information available, subject to NEST COR or NEST CTM approval:

a. When a NEST-maintained infrastructure resource (e.g., printing or email) is impaired or not available, those end users who have access rights to that resource shall be counted as affected. If the resource is accessible to a majority of end users (possibly all end users), then the number of end users in the organization to whom the resource is primarily
assigned shall be counted as affected.

b. NEST services – The number of end users who use an NEST-provided solution for their end-user services shall be counted as affected.

**Enterprise Service Desk (ESD)** – The initial and single point of contact for Enterprise IT Services support providing a unified interface between the customer and NASA IT service providers. The ESD is where end users’ Incidents and Service Requests are processed and routed to the Tier 2 contractors. The ESD provides both Tier 1 services and a Tier 0 (Self-Service) Web site. The Tier 0 site includes the service catalog.

**Entry Level** – Refers to the minimum or entry level printing capability in terms of “pages per minute (ppm)” required for a specified print device. Understanding that as hardware changes, this minimum or Entry Level performance standards (e.g. ppm) will increase.

**Failed Deployment** – A deployment that was started and not completed due to issue or error with deployment plan, steps, scripts, etc.

**Familiarization Training** – Training that acquaints the average skilled end user with the features, capabilities, configuration (either as OEM-configured or as Contractor-configured, as applicable) and optional components of the product or service.

**Federal information systems** – All information systems provided and/or operated under this contract and in support of this contract are Federal information systems. A federal information system is defined in NIST SP 800-37 (Revision 1), Guide for Applying the Risk Management Framework to Federal Information Systems and in 40 U.S.C., Sec. 11331, as an information system used or operated by a Federal agency, or by a contractor of a Federal agency or by another organization on behalf of a Federal agency.

**Greening** – The process of transforming IT products and services to be more environmentally friendly. The act of greening involves incorporating “green” products and processes into one’s work place. “Green” qualities include, but are not limited to, reduced toxicity, re-usability, energy efficiency, responsible packaging and labeling, recycled content, intelligent design, responsible manufacturing techniques, and reduction of personal environmental hazards.

**High Level** – Refers to the minimum or high level printing capability in terms of “pages per minute (ppm)” required for a specified print device. Understanding that as hardware changes, this minimum or High Level performance standards (e.g. ppm) will increase.

**Hot Spot** – Mobile Hot Spot is an ad hoc wireless access point that is created by a dedicated hardware device or a smartphone feature that shares the phone’s cellular data.

**Incident (ITIL® v3)** – An unplanned interruption to an IT Service or a reduction in the quality or IT security (e.g., notification or detection of a security violation or intrusion) of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident.

**Infection** – A software program capable of replicating itself and causing harm to either a computer system’s hosted data, functional performance, or networking throughput. Often referred to as a virus, infections include all types of malware such as a worm, trojan horse, spyware, dishonest adware, crimeware, and other malicious and unwanted software viruses that
intentionally enter an end user’s computer system to damage, destroy, or modify files and programs. Unaware of the Problem, the end user might spread the virus to other computers by infecting files on a network file system or a file system that is accessed by others.

**Information Systems** – The tools for and process of storing, managing, using and gathering of data and communications in an organization.

**Information Technology (IT)** – The hardware and software used to store, retrieve, and manipulate electronic information.

**Information Technology Infrastructure Library (ITIL®)** – A framework of good and best practices designed to promote quality computing services in the IT sector.

**Information Technology Service Management (ITSM)** – The system of processes, systems, and governance in place to help NASA structure and measure how it delivers IT services to its users.

**Initial Deployment Date** – Date installation was completed for new services or completion of refresh activity. Redeployment of a device does not reset the initial deployment date.

**Interoperability** – Ability of a computer system to run application programs from different vendors and to interact with other computers across local or wide-area networks regardless of their physical architecture and operating systems. Interoperability is feasible through hardware and software components that conform to open standards such as those used for the Internet.

**IT Infrastructure** – The sum of an organization’s IT related hardware, software, data, telecommunications, facilities, procedures, and documentation.

**IT Resources** – Any hardware or software or interconnected system or subsystem of equipment, that is used to process, manage, access, or store electronic information.

**Knowledge Article** – Items of knowledge, such as a policy, release notes, how-to, or FAQ. Each article exists within the ESD’s knowledge base, which is managed by one or more knowledge managers. Users can browse and search knowledge using a knowledge homepage or contextual search from other ServiceNow applications. The articles are used by support personnel for Tier 0/1/2 support.

**Least Privilege** – Allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

**Machine-to-Machine Wireless** – Wireless service that will enable users to obtain carrier data communications with potentially a variety of connected devices. Examples of M2M wireless uses 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. This capability is associated with the Internet of Things (IoT).

**Messaging** – Asynchronous collaboration capabilities enable a different time, different place interaction between collaborators. Asynchronous communications are not immediately received
or responded to by those involved (e.g. Emails, Data Sharing (Drop Box), social networking and message board forums which allow people to communicate on different schedules).

**Mobile Devices** – Are comprised of Cellular Devices (Cell Phones and Smartphones Cellular such as Androids and iPhones), Tablet Devices (as defined in the NASA-STD-2805, Minimum Hardware Configurations), Pager Devices, Mobile Hot Spot Devices, Cellular and Data Plan Service for Other Mobile Devices (Government-owned) and Machine-to-Machine Wireless Service.

**Mission Directorate** – One of NASA’s four primary business areas for implementing NASA’s mission and serving its customers. The four NASA Mission Directorates are: the Aeronautics Research Mission Directorate (ARMD), Exploration Systems Mission Directorate (ESMD), Science Mission Directorate (SMD), and Space Operations Mission Directorate (SOMD).

**NASA Data** – Any data and information, except for limited rights data or restricted software, which is produced or specifically used in the performance of a NASA contract.

**Near-site** – A business or other government agency affiliated with NASA that is within a ten (10)-mile perimeter of a NASA Center or Facility.

**Network Interface Card (NIC)** – An adapter card installed in a computer that enables it to connect to a network.

**Network Interface** – The physical, logical, and management connections where there is a distinct change in management responsibility or technical implementation. Network interfaces can occur between two distinct networks or between an end-user device and its supporting network.

**Network Printer** – A printer available for use by computing devices on a network. A network printer either has its own built-in network interface card or is connected to a computer on the network and shared.

**Off-site** – A business or other government agency affiliated with NASA that is outside of a ten (10)-mile perimeter of a NASA Center.

**On-site** – A business or other government agency affiliated with NASA that is located within the perimeter of the NASA Center.

**Optional Software** – Software available to customers subscribed to Software Load Services, but installed on request only.

**Outreach** – The act of extending training, information, services, and benefits to a wider section of the end-user population. The purpose of outreach is to promote and facilitate use of service capabilities to better support end-users’ mission success. Effective outreach expands end-users’ knowledge and understanding of, and generates interest in, services and service offerings.

**Pager systems** – Center-wide pager services, local or regional pager services, and national/international pager services necessary to support NASA requirements.

**Peripherals** – Devices (e.g., printers, scanners, plotters, modems, and external hard disks) attached to individual desktops, laptops, or workstations.
Preventable Incidents under the terms of the Contract – Incidents resulting from the Contractor’s lack of patch deployment.

Print Services – Include hardware, maintenance, support, and network connectivity, and can interface with authorized computers to provide, at a minimum, complete print functionality.

Problem (ITIL® v3) – A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is followed to provide further investigation.

Refresh Cycle – Period of time in months from initial deployment of an asset to the end of life and planned replacement.

Responsiveness – The speed with which the Contractor responds to an Incident.

Return To Service (RTS) – In ITIL® v3 known as Restoration of Service, the restoration of an end user’s device to full operability when an Incident occurs that renders a NEST seat unstable or inoperable. RTS 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 field services and any remote management. RTS is the primary objective of Incident Management.

Return to Service timeframe – The time from detection of an Incident until the service is fully restored to the end user.

Restore – Taking action to return an IT service to the users after repair or recovery from an incident (see RTS above).

Sanitization (sanitize) – The process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device.

Scheduled Outage – Any planned activity that impacts the end user’s ability to access NEST services. A scheduled outage is considered downtime if all affected end users were not notified at least 3 days in advance. Unless directed by the Government to conduct maintenance or testing, an outage during Business hours shall be counted as downtime.

Security Management (ITIL® v3) – The structured fitting of security in the management organization with a focus on guaranteeing the safety of information and placing value on protecting the confidentiality, integrity, and availability of information. The goal of Security Management is to meet the security requirements of Service Level Agreements, contracts, legislation, and externally imposed policies.

Security Operations Center (SOC) – The NASA SOC monitors activity and events in the NASA environment to ensure that anomalous behavior is detected, identified, classified, and acted upon where appropriate. Security engagements are co-managed by the SOC and the Contractor where actionable behavior by each is recommended in the event of malicious activities.

Server Administration – Services provided in the operation and maintenance of a server. This includes services such as installation of a new server and additional hardware, installation and upgrade of software applications and network operating system, and configuration of hardware
and software. This also includes account management, backup and restore, performance monitoring and tuning, security monitoring, Problem tracking, and error detection.

**Service Asset and Configuration Management (SACM)** – The process responsible for ensuring that Configuration Items (CI) required to deliver services are properly controlled, and that accurate and reliable information about those CIs is readily available. This information includes details of how the CIs have been configured and the relationships between assets.

**Service Desk** – The Single Point of Contact between the Service Provider and the end users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the end users. The primary purpose of a Service Desk is to manage, coordinate, and resolve Incidents as quickly as possible and to ensure that no ticket is lost, forgotten, or ignored. Under the Contract, the Contractor’s Tier 2/3 service desk will respond to reported Incidents, Problems, and Service Requests originating from the Enterprise Service Desk (ESD).

**Service Level Agreement (SLA) (ITIL® v3)** – An agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers.

**Service Level (ITIL® v3)** – Measured and reported achievement against one or more Service Level Targets. The term Service Level is sometimes used informally to mean Service Level Target.

**Service Option** – The end-user configurable components that define a particular service provided by the Contractor.

**ServiceNow** – The ESD instance of ServiceNow is the government’s ITSM system.

**Shared Peripherals** – Peripheral devices available to the end user through a local area network. This includes printers, multi-functional devices (MFDs), scanners, plotters, and modems.

**Smartcard** – A Smartcard is a card the size and shape of a standard credit card that is used to access IT resources. Imbedded in the plastic is a complete microprocessor, memory, and input/output (I/O) interface. To use a Smartcard to access an IT resource, you need a Smartcard reader—a small device into which you insert the Smartcard—and the Personal Identification Number (PIN) that is associated with the Smartcard. Smartcards can provide a level of security higher than software-only implementations.

**Software Release** – The date that a software developer makes their software product publicly available. This date is often used in determining when a software product is deployed to end-user computing devices and other IT devices.

**Software Subscriptions by Title** – Software available to customers only via title specific subscription.

**Straight line depreciation** – The simplest and most commonly used method of determining the value that an asset will lose each month over its useful life. Straight line depreciation is calculated by taking the purchase or acquisition price of an asset, subtracting the expected salvage value, and dividing the result by the useful life of the asset.
**System Administration** – Duties performed by a system administrator (also known as “admin,” “sys admin,” and “site admin”), such as monitoring security, performing configuration, managing allocation of user accounts and passwords, monitoring disk space and other resource use, and setting up new user accounts, hardware, and software.

**Task Order Manager** – As Task Orders are awarded, Task Order Managers (TOM) will be appointed by the COR. TOM’s will obtain performance information for their functional area based on the surveillance methods identified in Attachment I-3, *Service Level Agreements* (SLAs), Attachment I-20, *Quality Assurance Surveillance Plan (QASP)*, or other surveillance methods as appropriate.

**Technical Monitor Assessment** – These reports will address and fully substantiate strong and weak points and all significant issues, problems, and concerns that should be brought to the attention of the ATEB and Contractor.

**Telework** – The term ‘telework’ or ‘teleworking’ refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee’s position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.

**Tiers** – Tier 0 = Self-Service, Tier 1 = ESD support, Tier 2 = NEST support, Tier 3 = NEST vendor or civil servant support.

**Tier 2 NEST Service Desk** – A NEST-staffed second tier service desk support where calls/Incident requests from NEST end users are routed from the Enterprise Service Desk (Tier 1 Service Desk) because no specialist with the knowledge of the solution and ability to implement the solution is available at that Tier 1 Service Desk.

**Traveler (CONUS and OCONUS)** – An individual who is traveling or who often travels from the location from which the employee would otherwise work.

**Unsubscription** – Request to decommission a deployed service.

**Update/Upgrade** – The replacement of a software program or hardware device with a more recently released version that provides better performance or newer functionality.

**Useful life** – The time until the asset transition value of an asset has reached zero or the asset with residual value is no longer functional.

**Vital Records** – Records essential for maintaining the continuity of Federal Government activities during a national emergency. These records consist of two categories: (1) emergency operating records, which outline the essential functions of the Government for the duration of emergency conditions, and (2) rights and interests records, which are required for the preservation of the rights and interests of individual citizens and the Government. (See NPD 1440.6, *NASA Records Management*.)

**Wipe and Load** – The act of erasing all information on all of the NEST-supported hard drives associated with an NEST seat and bringing the seat back to the current, fully functional baseline configuration.
**Workaround** – A method of addressing an Incident or Problem, either as a temporary fix or through access to an alternative service.

**Workstation** – A networked or standalone computer normally used for calculation or graphics-intensive applications. A workstation includes one or more CPUs, monitor, keyboard, and a mouse or other screen manipulation device.

**Zero Touch** – An approach that allows devices to be provisioned and configured automatically, eliminating most of the manual labor involved with deploying them.