WORKING DRAFT OF TERMS AND CONDITIONS & FACTOR FOR EVALUATION FOR IT SCHEDULE 70 CLOUD COMPUTING SERVICES SIN

Disclaimer: This document is a **working draft** issued for comment to industry, meant to seek feedback about the overall approach to a Cloud Special Item Number (SIN) on IT Schedule 70. There is no guarantee that GSA will issue a Request For Proposal (RFP) or make an award. The Terms and Conditions and Factor for Evaluation cited in this document are not final and do not represent GSA's ultimate position on the Cloud Computing Services SIN. This document was developed taking into consideration the input received from industry on the Request for Information (RFI) issued on July 9, 2014.

GSA is seeking feedback from industry on this document. We welcome high level feedback such as your agreement or disagreement with the overall draft terms and conditions documentation; suggestions for meeting the goals of the Cloud SIN; or suggested wording when articulating alternatives. While reviewing the document and offering your valuable feedback, please consider the following questions:

1. Do the Terms and Conditions appear flexible, fair and competitive, while retaining the intent of having vetted cloud services?
2. Do the Terms and Conditions support the ability for customers to easily locate and distinguish cloud computing services from other IT services and conveniently view services by relevant criteria?
3. Will the Terms and Conditions support a broad range of potential industry partners, including cloud service providers and resellers, small and large businesses?
4. Do the Terms and Conditions address the industry best practices and standards?
5. Are there additional areas that we need to address in the terms and conditions?
6. Does the Factor for Evaluation provide a clear and straightforward manner of evaluating cloud computing services?

GSA appreciates the feedback received through the RFI results and looks forward to working with industry on the next iteration of preparing for a new Cloud Computing Services SIN on Schedule 70.

Please submit feedback or questions by sending an email to cloud-sin-rfi@gsa.gov. More information about the proposed SIN can be found at the Cloud SIN webpage.

The draft Terms and Conditions begin on the following page. The draft Factor for Evaluation is on page 16.

TERMS AND CONDITIONS APPLICABLE TO CLOUD COMPUTING SERVICES (SPECIAL ITEM NUMBER XXX-XX)

*****NOTE: If offering related Cloud Computing IT Professional Services over and above initial onboarding and training, reference SIN 132-51, per Guidance on Professional services below.*

*****NOTE: The motivation of adding this new SIN is to present a clear way for contractors to provide cloud services according to NIST definitions and principles within the scope of today's technology and standards with a secondary goal of accommodating ongoing technical advances in cloud computing.*

1. SCOPE

The prices, terms and conditions stated under Special Item Number 132-XX Cloud Computing Services apply exclusively to Cloud Computing Services within the scope of this Information Technology Schedule.
This SIN provides ordering activities with access to technical services that run in cloud environments and meet the NIST Essential Characteristics. Services relating to or impinging on cloud that do not meet all NIST essential characteristics should be listed in other GSA SINs or categories.

Sub-categories in scope are the three NIST Service Models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Offerors may submit multiple cloud offerings. For each proposed cloud service, offerors may select the single sub-category that best fits their offering; see service model guidance. For each proposed cloud service, offerors may not select multiple sub-categories that apply to a single cloud service. Sub-category selection within this SIN is optional and new cloud computing technologies not otherwise included in the aforementioned three sub-categories may be included without a sub-category selection so long as they comply with the essential characteristics of cloud computing as outlined by NIST.

See Table 1 for a representation of the scope and sub-categories.

Table 1: Cloud Computing Services SIN

SIN Description	Optional Sub-Categories (Select One Only) [1]
• Commercially available cloud computing services • Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing • Open to all deployment models (private, public, community or hybrid), vendors specify deployment models	1. **Software as a Service (SaaS):** Consumer uses provider's applications on cloud infrastructure. Does not manage/control infrastructure. 2. **Platform as a Service (PaaS):** Consumer deploys applications onto cloud infrastructure using provider-supplied tools. Has control over deployed applications but not infrastructure. 3. **Infrastructure as a Service (IaaS):**

[1] Offerors may optionally select the single sub-category that best fits their offering, per Service Model Guidance, or select no sub-category if the offering does not fit an existing NIST service model.

SIN Description	Optional Sub-Categories (Select One Only) [1]
• Will cover future cloud technology not otherwise covered by current NIST cloud definitions	Consumer provisions computing resources. Has control over OS, storage, and deployed applications, but does not manage the infrastructure.

2. DESCRIPTION OF CLOUD COMPUTING SERVICES AND PRICING

NOTE TO CONTRACTORS: The information provided below is designed to assist Contractors in qualifying cloud computing services for this SIN and providing complete descriptions and pricing information. This language should NOT be printed as part of the Information Technology Schedule Pricelist; instead, Contractors should respond to each service requirement as it relates to each cloud computing service offered under the contract. There is guidance provided in subsequent sections of the Terms and Conditions to assist in determining how to meet these requirements. This section delineates requirements for submitting a proposal for the Cloud SIN, as well as requirements that apply to Task Orders

a. Service Description Requirements for Listing Contractors

Table 2 summarizes contractor-provided description requirements for services proposed under the Cloud SIN. The description requirements fall into two mandatory reporting types which will be evaluated according to type:

- "**Mandatory – Evaluated for Content**" must be complete and must additionally meet specific substantive evaluation criteria. Each NIST Essential Characteristic, for example, must be complete and adequate according to evaluation criteria.
- "**Mandatory, Evaluated for Completeness**" will be evaluated for completeness but need not meet specific additional content evaluation criteria. For example contractors must provide full and complete information on FedRAMP status and plans, but the SIN is not limited to any specific FedRAMP status.

In addition there are two "Optional" reporting descriptions which exist to provide convenient service selection by relevant criteria:

- The NIST Service Model provides primary sub-categories for the Cloud SIN and is strongly encouraged, but not required. The Service Model based sub-categories provide this SIN with a structure to assist ordering activities in locating and comparing services of interest. Contractors may optionally select the single service model most closely corresponding to their service offering.
- Service Model sub-categorization is optional in order to accommodate future new service models while covering the vast majority of current services.
- The Professional Services description is optionally available for those contractors who wish to associate their existing GSA professional services listings with the corresponding Cloud Services under this SIN.

A number of the description items are likely to change over time. It is the Contractor's responsibility to ensure that the information in the listing is updated to be current within 20 business days of any change in description or status, for example a change in FedRAMP status, HIPAA certification, etc.

Table 2: Cloud Service Description Requirements

#	Description Requirement	Reporting Type	Instructions
1	Provide a brief written description of how the cloud service proposed satisfies each individual essential NIST Characteristic	Mandatory – Evaluated for Content	The cloud service technology must be capable of satisfying each of the five NIST essential Characteristics. See 'GUIDANCE FOR CONTRACTORS: NIST Essential Characteristics' for detailed direction.
2	Optionally select the most appropriate NIST service model that will be the designated sub-category, or may select no sub-category.	Optional	Contractor may select a single NIST Service model to sub-categorize the service. Sub-category selection is optional but recommended. See 'GUIDANCE FOR CONTRACTORS: NIST Service Model' for detailed direction on how to best categorize the service for the NIST IaaS, PaaS, and SaaS service models
3	Provide the most appropriate deployment model associated with each proposed cloud service	Mandatory – Evaluated for Completeness	The Contractor shall document at least one deployment model (e.g. Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud) conforming to the definitions in The NIST Definition of Cloud Computing SP 800-145 page 3. See 'GUIDANCE FOR CONTRACTORS: NIST Deployment Model' for detailed direction
4	FISMA or Information Assurance/Security Requirement Certifications	Mandatory – Evaluated for Completeness	List relevant security certifications or standards met by the service. See 'GUIDANCE FOR CONTRACTORS: FISMA/ Information Assurance and Security' for detailed direction
5	FedRAMP Status	Mandatory – Evaluated for Completeness	List the current FedRAMP status of the service. See 'GUIDANCE FOR CONTRACTORS: FedRAMP Status Reporting' for detailed direction
6	Privacy and Accessibility	Mandatory – Evaluated for Completeness	Indicate any agencies certifying that the service is in compliance with policies on Personally Identifying Information, Accessibility and additional optional compliances such as HIPAA. See 'GUIDANCE FOR CONTRACTORS: Privacy and Accessibility' for detailed direction
7	Geographic Requirements	Mandatory – Evaluated for Completeness	Certify capabilities for geographic restriction on data and processing location. See 'GUIDANCE FOR CONTRACTORS: Geographic Requirements' for detailed direction
8	Data Ownership and Retrieval	Mandatory – Evaluated for Content	Describe Ordering Activity ownership of data and capabilities for data retrieval. See 'GUIDANCE FOR CONTRACTORS: Data Ownership and Retrieval' for detailed direction
9	Data Center Distribution	Mandatory –	Describe available data center locations and capabilities

#	Description Requirement	Reporting Type	Instructions
		Evaluated for Completeness	to distribute processing and data across multiple centers. See 'GUIDANCE FOR CONTRACTORS: Data Center Distribution' for detailed direction
10	Related Professional Service Listings	Optional	Optionally list existing GSA Professional Service contracts supporting the service with web link to the relevant description in GSA systems. See 'GUIDANCE FOR CONTRACTORS: Related Professional Services' for detailed direction

b. Pricing of Cloud Computing Services

As commercial cloud computing services have various pricing models with limited standardization across industry, the primary requirement for cloud computing services is alignment with NIST essential characteristics. All pricing models must have the core capability to meet the NIST Essential Cloud Characteristics, particularly with respect to on-demand self-service, while allowing alternate variations at the task order level at agency discretion, pursuant to the guidance on NIST Essential Characteristics.

3. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

a. Rights in Data

The Contractor shall comply FAR 52.227-14 RIGHTS IN DATA – GENERAL and with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character and any additional terms and conditions that are added at the task order level to supplement 52.227-14.

b. Acceptance Testing

If requested by the ordering activity the Contractor shall provide acceptance test plans and procedures for ordering activity approval. The Contractor shall perform acceptance testing of the systems for ordering activity approval in accordance with the approved test procedures.

c. Warranty

The Contractor shall provide a warranty covering each Contractor-provided cloud computing service or ancillary physical equipment. The minimum duration of the warranty shall be the duration of the manufacturer's commercial warranty for the item listed below:
Insert commercial warranty.
The warranty shall commence when the user's service is activated or when any approval processes are successfully completed, whichever comes later.
The Contractor, by repair or replacement of the defective service or ancillary physical equipment, shall complete all warranty services within five working days of notification of the defect. Warranty service shall be deemed complete when the user has access to the repaired or replaced service.

d. Training

If training is provided commercially the Contractor shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system. If there is a separate charge, indicate below.

4. RESPONSIBILITIES OF THE ORDERING ACTIVITY

The Ordering Activity is responsible for indicating cloud computing services requirements unique to the Ordering Activity. Additional requirements should be enhancements, clarifications or specifications of existing SIN requirements, but should not contradict existing SIN or IT Schedule 70 Terms and Conditions. Ordering Activities should include (as applicable) Terms & Conditions to address Pricing, Security, Data Ownership, Geographic Restrictions, Privacy, SLAs, etc.

a. Ordering Activity Information Assurance/Security Requirements

i. The Ordering Activity is responsible for ensuring to the maximum extent practicable that each requirement issued is in compliance with the Federal Information Security Management Act (FISMA) as applicable

ii. The Ordering Activity shall assign a required impact level (per Federal Information Processing Standards Publication 199 & 200 (FIPS 199, *"Standards for Security Categorization of Federal Information and Information Systems"*) (FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*") for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work. Evaluations shall consider the extent to which each proposed service accommodates the necessary security controls based upon the assigned impact level. The Contractor awarded SIN XXX-XX must be capable of meeting at least the minimum security requirements assigned against a low-impact information system in each CIA assessment area (per FIPS 200) and must detail the FISMA capabilities of the system in each of CIA assessment area.

iii. Agency level FISMA certification, accreditation, and evaluation activities are the responsibility of the ordering activity. The Ordering Activity reserves the right to independently evaluate, audit, and verify the FISMA compliance for any proposed or awarded Cloud Computing Services.

iv. Ordering Activities bear the final responsibility for complying with FedRAMP requirements based on both the information supplied by the contractor (see Contractor Responsibilities) and their own efforts. The Ordering Activity is responsible for assessing the FedRAMP status of the service, complying with and making a risk-based decision to grant an Authorization to Operate (ATO) for the cloud computing service, and continuous monitoring. Per the OMB memo published on December 8, 2011, all low and moderate impact cloud services leveraged by more than one office or agency must comply with FedRAMP requirements by June 2014.

b. Delivery Schedule

The Ordering Activity shall specify the delivery schedule as part of the initial requirement. The Delivery Schedule options are found in *Information for Ordering Activities Applicable to All Special Item Numbers*, paragraph 6. *Delivery Schedule.*

c. Interoperability

Ordering Activities are responsible for identifying interoperability requirements. Interfaces, including application program interfaces (APIs), endpoints and implemented applicable standards may be identified as interoperable on the basis of participation in a sponsored program acceptable to the Ordering Activity, specific function point interoperation with specified external services, or both. Ordering activities should clearly delineate requirements for API implementation and standards conformance.

d. Performance of Cloud Computing Services

The Ordering Activity should clearly indicate any custom minimum service levels, performance and scale requirements as part of the initial requirement.
The Ordering Activity should specify any specific data center location requirements.
The Contractor shall respond with proposed capabilities to Ordering Activity performance specifications or indicate that only standard specifications are offered. In all cases the Contractor shall clearly indicate standard service levels, performance and scale capabilities.
The Contractor shall provide appropriate cloud computing services on the date and to the extent and scope agreed to by the Contractor and the ordering activity.

e. Reporting

The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of the initial requirement.
The contractor shall respond to ordering activity requirements and specify general reporting capabilities available for the Ordering Activity to verify performance, cost and availability.
In accordance with commercial practices, the Contractor may furnish the ordering activity/user with a monthly summary ordering activity report.

5. GUIDANCE FOR CONTRACTORS

This section offers guidance for interpreting the Contractor Description Requirements in Table 2, including and especially the NIST characteristics, service models and deployment models.
Services qualifying for listing as cloud computing services under this SIN must substantially satisfy the essential characteristics of cloud computing as documented in the NIST Definition of Cloud Computing SP 800-145[2]. Contractor-specific definitions of cloud computing characteristics and models or significant variances from the NIST essential characteristics are discouraged and will be considered outside the scope of this SIN as detailed in Evaluation Criteria. The NIST Characteristics are the guiding principles that will be applied to this Cloud SIN to determine alignment with a true cloud offering.

Contractors submitting services for listing under this SIN are encouraged to select a sub-category for each service proposed under this SIN with respect to a single principal NIST cloud service model that most aptly characterizes the service. Service model categorization is optional.

In addition, Contractors must select deployment models corresponding to each way the service can be deployed. Multiple deployment models are permitted but at least one must be selected.

Both service and deployment model sub-categories must accord with NIST definitions, and guidance is offered in this document on making the most appropriate selection.

Contractor-specific or unique service or deployment models are strongly discouraged in order to provide consistent categorization under this SIN, see evaluation criteria.

a. NIST Essential Characteristics

NIST's essential cloud characteristics provide a consistent metric for whether a service is eligible for inclusion in this SIN. It is understood that due to legislative, funding and other constraints that

[2] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

government entities cannot always leverage a cloud service to the extent that all NIST essential characteristics are being deployed. However for the purposes of the Cloud SIN, meeting the NIST essential characteristics is concerned primarily with whether the underlying capability of the commercial service is available, whether or not the ordering activity actually requests or implements the capability. The guidance in Table 3 offers examples of how services might or might not be included based on the essential characteristics, and how a contractor should interpret the characteristics in light of current government contracting processes.

Table 3: Guidance on Meeting NIST Essential Characteristics

Characteristic	Intent and Clarification	Guidance
On-demand self-service	• Ordering activities can directly provision services without requiring contractor intervention. • This characteristic is typically implemented via a service console or programming interface for provisioning	Government procurement guidance varies on how to implement on-demand provisioning at this time. Ordering activities approach on-demand in a variety of ways, including "not-to-exceed" limits, requirements contracts or imposing monthly or annual payments on what are essentially on demand services. Until clear procurement guidance is available, services under this SIN must be capable of true on-demand self-service and ordering activities and contractors must negotiate how they implement on demand capabilities in practice: • Ordering activities must specify their procurement approach and requirements for on-demand service • Contractors must propose how they intend to meet the approach • Contractors must certify that on-demand self-service is technically available for their service should procurement guidance become available.
Broad Network Access	• Ordering activities are able to access services over standard agency networks • Service can be accessed and consumed using standard devices such as browsers, tablets and mobile phones	• Broad network access must be available without significant qualification. • Contractors must specify any ancillary activities, services or equipment required to access cloud services. For example a private cloud might require an ordering activity to purchase or provide a dedicated router, etc. which is acceptable but should be indicated by the contractor.
Resource Pooling	• Pooling distinguishes cloud services from offsite hosting. • Ordering activities draw resources from a common pool maintained by the	• Contractors must manage a pool of resources and an automated means for the ordering activity to dynamically allocate them. • Manual allocation, e.g. manual operations at a physical server farm where contractor staff configure servers in response to ordering

Characteristic	Intent and Clarification	Guidance
	contractor • Resources may have general characteristics such as regional location	activity requests, does not meet this requirement • Similar concerns apply to software and platform models; automated provisioning from a pool is required • Ordering activities may request dedicated physical hardware, software or platform resources for a private deployment model. However the resources must be drawn from a common pool and automatically allocated on request.
Rapid Elasticity	• Rapid provisioning and de-provisioning commensurate with demand	• Rapid elasticity is a specific demand-driven case of self-service • Procurement guidance for on-demand self-service applies to rapid elasticity as well, i.e. rapid elasticity must be technically available but ordering activities and contractors may mutually negotiate other contractual arrangements for procurement and payment. • 'Rapid' should be understood as measured in minutes and hours, not days or weeks. • Elastic capabilities by manual request, e.g. a console operation, are required. • Automated elasticity which is driven dynamically by system load, etc. is optional. Contractors must specify whether automated demand-driven elasticity is available and the general mechanisms that drive the capability.
Measured Service	• Measured service should be understood as a reporting requirement that enables an ordering activity to control their use in cooperation with self service	• Procurement guidance for on-demand self-service applies to measured service as well, i.e. rapid elasticity must be technically available but ordering activities and contractors may mutually designate other contractual arrangements. • Regardless of specific contractual arrangements, reporting must indicate actual usage, be continuously available to the ordering activity, and provide meaningful metrics appropriate to the service measured • Contractors must specify that measured service is available and the general sort of metrics and mechanisms available

b. NIST Service Model

The Contractor may optionally document the service model of cloud computing (e.g. IaaS, PaaS, SaaS, or a combination thereof, that most closely describes their offering, using the definitions in The NIST Definition of Cloud Computing SP 800-145. The following guidance is offered for the proper selection of service models.

NIST's service models provide this SIN with a set of consistent sub-categories to assist ordering activities in locating and comparing services of interest. Service model is primarily concerned with the nature of the service offered and the staff and activities most likely to interact with the service. Contractors should select a single service model most closely corresponding to their proposed service based on the guidance below. It is understood that cloud services can technically incorporate multiple service models and the intent is to provide the single best categorization of the service.

Contractors should take care to select the NIST service model most closely corresponding to each service offered. Contractors should not invent, proliferate or select multiple cloud service model sub-categories to distinguish their offerings, because ad-hoc categorization prevents consumers from comparing similar offerings. Instead vendors should make full use of the existing NIST categories to the fullest extent possible.

For example, in this SIN an offering branded by a contractor as "Storage as a Service" would be properly characterized as Infrastructure as a Service (IaaS), storage being a subset of infrastructure. Services branded as "LAMP as a Service" or "Database as a Service" would be properly characterized under this SIN as Platform as a Service (PaaS), as they deliver two kinds of platform services. Services branded as "Travel Facilitation as a Service" or "Email as a Service" would be properly characterized as species of Software as a Service (SaaS) for this SIN. However, contractors can and should include branded descriptions of the service in the full descriptions of the service's capabilities.

When choosing between equally plausible service model sub-categories, contractors should consider several factors:

1) **Visibility to the Ordering Activity**. The service model sub-categories in this SIN exist to help ordering activities match their requirements with service characteristics. Contractors should select the most intuitive and appropriate service model from the point of view of an ordering activity.
2) **Primary Focus of the Service**. Services may offer a mix of capabilities that span service models in the strict technical sense. For example, a service may offer both IaaS capabilities for processing and storage with some PaaS capabilities for application deployment, or SaaS capabilities for specific applications. In a service mix situation the contractor should select the service model that is their primary focus.
3) **Ordering Activity Role**. Contractors should consider the operational role of the ordering activity's primary actual consumer or operator of the service. For example services most often consumed by system managers are likely to fit best as IaaS; services most often consumed by application deployers or developers as PaaS, and services most often consumed by business users as SaaS.
4) **Lowest Level of Configurability.** Contractors can consider IaaS, PaaS and SaaS as an ascending hierarchy of complexity, and select the model with the lowest level of available ordering activity interaction. As an example, virtual machines are an IaaS service often bundled with a range of operating systems, which are PaaS services. The ordering activity usually has access to configure the lower level IaaS service, and the overall service should be considered IaaS. In cases where the ordering activity cannot configure the speed, memory, network configuration, or any other aspect of the IaaS component, consider categorizing as a PaaS service.

Cloud management and cloud broker services should be categorized based on their own characteristics and not those of the other cloud services that are their targets. Management and broker services typically fit the SaaS service model, regardless of whether the services they manage are SaaS, PaaS or IaaS. Use Table 3 to determine which service model is appropriate for the cloud management or cloud broker services, or, alternately choose not to select a service model for the service.

The guidance in Table 3 offers examples of how services might be properly mapped to NIST service models and how a contractor should interpret the service model sub-categories.

Table 3: Guidance on Mapping to NIST Service Models

Service Model	Guidance
Infrastructure as a Service (IaaS)	Select an IaaS model for service based equivalents of hardware appliances such as virtual machines, storage devices, routers and other physical devices. • IaaS services are typically consumed by system or device managers who would configure physical hardware in a non-cloud setting • The principal customer interaction with an IaaS service is configuration, equivalent to configuring a physical device. Examples of IaaS services include virtual machines, object storage, disk block storage, network routers and firewalls, software defined networks. Gray areas include services that emulate or act as dedicated appliances and are directly used by applications, such as search appliances, security appliances, etc. To the extent that these services or their emulated devices provide direct capability to an application they might be better classified as Platform services (PaaS). To the extent that they resemble raw hardware and are consumed by other platform services they are better classified as IaaS.
Platform as a Service (PaaS)	Select a PaaS model for service based equivalents of complete or partial software platforms. For the purposes of this classification, consider a platform as a set of software services capable of deploying all or part of an application. • A complete platform can deploy an entire application. Complete platforms can be proprietary or open source • Partial platforms can deploy a component of an application which combined with other components make up the entire deployment • PaaS services are typically consumed by application deployment staff whose responsibility is to take a completed agency application and cause it to run on the designated complete or partial platform service • The principal customer interaction with a PaaS service is deployment, equivalent to deploying an application or portion of an application on a software platform service. Examples of complete PaaS services include: • A Linux/Apache/MySQL/PHP (LAMP) platform ready to deploy a customer PHP application, • a Windows .Net platform ready to deploy a .Net application, • A custom complete platform ready to develop and deploy an customer application in a proprietary language • A multiple capability platform ready to deploy an arbitrary customer application on

Service Model	Guidance
	a range of underlying software services. The essential characteristic of a complete PaaS is defined by the customer's ability to deploy a complete custom application directly on the platform. PaaS includes partial services as well as complete platform services. Illustrative examples of individual platform enablers or components include: • A database service ready to deploy a customer's tables, views and procedures, • A queuing service ready to deploy a customer's message definitions • A security service ready to deploy a customer's constraints and target applications for continuous monitoring The essential characteristic of an individual PaaS component is the customer's ability to deploy their unique structures and/or data onto the component for a partial platform function. Note that both the partial and complete PaaS examples all have two things in common: • They are software services, which offer significant core functionality out of the box • They must be configured with customer data and structures to deliver results As noted in IaaS, operating systems represent a grey area in that OS is definitely a platform service, but is typically bundled with IaaS infrastructure. If your service provides an OS but allows for interaction with infrastructure, please sub-categorize it as IaaS. If your service "hides" underlying infrastructure, consider it as PaaS.
Software as a Service (SaaS)	Select a SaaS model for service based equivalents of software applications. • SaaS services are typically consumed by business or subject-matter staff who would interact directly with the application in a non-cloud setting • The principal customer interaction with a SaaS service is actual operation and consumption of the services the software application provides. Some minor configuration may be available, but the scope of the configuration is limited to the scope and then the permissions of the configuring user. For example an agency manager might be able to configure some aspects of the application for their agency but not all agencies. An agency user might be able to configure some aspects for themselves but not everyone in their agency. Typically only the contractor would be permitted to configure aspects of the software for all users. Examples of SaaS services include email systems, business systems of all sorts such as travel systems, inventory systems, etc., wiki's, websites or content management systems, management applications that allow a customer to manage other cloud or noncloud services, and in general any system where customers interact directly for a business purpose. Gray areas include services that customers use to configure other cloud services, such as cloud management software, cloud brokers, etc. In general these sorts of systems should be considered SaaS, per guidance in this document.

a. Deployment Model

Deployment models (e.g. private, public, community, or hybrid) are not restricted at the SIN level and any specifications for a deployment model are the responsibility of the Ordering Activity.

Multiple deployment model selection is permitted, and at least one model must be selected. The guidance in Table 4 offers examples of how services might be properly mapped to NIST deployment models and how a contractor should interpret the deployment model sub-categories. Contractors should take care to select the range of NIST deployment models most closely corresponding to each service offered.

Table 4: Guidance for Selecting a Deployment Model

Deployment Model	Guidance
Private Cloud	The service is provided exclusively for the benefit of a definable organization and its components; access from outside the organization is prohibited. The actual services may be provided by third parties, and may be physically located as required, but access is strictly defined by membership in the owning organization.
Public Cloud	The service is provided for general public use and can be accessed by any entity or organization willing to contract for it.
Community Cloud	The service is provided for the exclusive use of a community with a definable shared boundary such as a mission or interest. As with private cloud, the service may be in any suitable location and administered by a community member or a third party.
Hybrid Cloud	The service is composed of one or more of the other models. Typically hybrid models include some aspect of transition between the models that make them up, for example a private and public cloud might be designed as a hybrid cloud where events like increased load permit certain specified services in the private cloud to run in a public cloud for extra capacity, e.g. bursting.

b. FISMA/Information Assurance and Security

FISMA and other Information and Assurance and Security compliance is ultimately an Ordering Activity responsibility. In order to assist Ordering Activities in assessing the current compliance status of the service, contractor shall specify each FISMA or other relevant security certification or standard met by the service. This information is intended to advise the Ordering Activity on existing compliances for the service.

c. FedRAMP Status Reporting

The contractor shall specify type and date of FedRAMP authorization available for their service:

- In cases of current authorizations contractor shall list effective date, expiry / reassessment date and type of authorization, e.g. JAB Provisional Authorization, Agency Authorization, Cloud Provider Supplied documentation with third party assessment, or other forms authorized by the FedRAMP program office.
- In cases of lapsed authorizations, contractor shall list expiry date and type of authorization

- Where an authorization is in process with FedRAMP contractor shall list type of authorization, initiation date, current status and expected completion.
- Where no authorization exists, contractor shall state how they will meet FedRAMP requirements, (e.g. apply to JAB, partner with agency or initiate independent process), and the expected funding strategy, (e.g. cost built into service, agency pays, contractor pays separately).

d. Privacy and Accessibility

The contractor shall specify the privacy and accessibility characteristics of their service.

For privacy:

- An attestation that the service is capable of safeguarding Personally Identifiable Information (PII), in accordance with NIST SP 800-1223 and OMB memos M-06-164 and M-07-165. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy.
- An optional list of agencies who have certified that the service provides such PII protections and dates of certification
- Whether or not the service is HIPAA compliant, and the date of compliance

For accessibility:

- An attestation that the service provides accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).
- An optional list of agencies who have certified that the service provides such Section 508 accessibility and date of certification.

e. Geographic Requirements Guidance

Ordering activities are responsible for specifying any geographic requirements at the task order level. The contractor shall specify their capabilities to meet geographic requirements if imposed by the ordering activity:

- Certify whether all service data, processes and related artifacts can be confined to the United States and its territories on request.

---

[3] NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)",

[4] OMB memo M-06-16: Protection of Sensitive Agency Information http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf

[5] OMB Memo M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

- Certify whether all service data, processes and related artifacts can be confined to the continental United States (CONUS) on request. .

f. Data Ownership and Retrieval

The contractor shall certify that:

- The Government (Ordering Activity) retains ownership of all data, government created scripts/applications specific to the integration, and any government provided resources including hardware or virtual machines created with individual task orders.
- The Government (Ordering Activity) retains ownership of user-loaded software and any application or product that is developed.

The contractor shall transfer data either on demand or in case of order termination for any reason. Delivered data shall conform to an industry standard format capable of being transported to other systems using a mutually agreed to electronic format. The contractor shall specify the format(s) data will be provided in.

g. Data Center Distribution

The contractor shall specify the distribution, availability and approximate locations of data centers and the degree to which data centers may be considered to be independent for continuity of operations purposes.

h. Related Professional Services

Contractors may detail professional services in this SIN limited to assisting offering activities with initial setup, training and access to the services.

Additional ongoing professional services related to the offering such as integration, migration, and other cloud professional services are not in scope of this SIN and they should be listed on the appropriate GSA professional services schedule.

Ordering activities may assemble packages of cloud services and related ongoing professional services by specifying a combination of cloud SIN and related professional service listings in their solicitations. In order to make related professional services visible at the Cloud SIN level and facilitate the process for ordering activities, contractors are encouraged to list GSA references or links for any ongoing professional services associated with the cloud service in the Related Professional Services area.

WORKING DRAFT OF FACTORS FOR EVALUATION FOR IT SCHEDULE 70 CLOUD COMPUTING SERVICES SIN

The following technical evaluation factor would be in addition to those outlined in CI-FSS-152 ADDITIONAL EVALUATION FACTORS and would apply solely to the Cloud Computing Services SIN. A template will be provided at the time of solicitation refresh to complete the requested documentation.

FACTOR - Cloud Computing Services Adherence to Essential Cloud Characteristics

Within a two page limitation for each cloud service provided, provide a description of how the cloud computing service meets each of the five essential cloud computing characteristics as defined in described in National Institute of Standards and Technology (NIST) Special Publication 800-145 and subsequent versions of this publication. This standard specifies the definition of cloud computing for the use by Federal agencies. The cloud service technology must be capable of satisfying each of the five NIST essential Characteristics as follows:

- On-demand self-service
- Broad network access
- Resource Pooling
- Rapid Elasticity
- Measured Service

For the purposes of the Cloud Computing Services SIN, meeting the NIST essential characteristics is concerned primarily with whether the underlying capability of the commercial service is available, whether or not an ordering activity actually requests or implements the capability.