TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF CLOUD COMPUTING SERVICES (SPECIAL ITEM NUMBER 132 40)

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

*******NOTE: This new SIN presents a clear way for Contractors to provide cloud computing 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.***

TERMS AND CONDITIONS

Note: These terms are in addition to those described in Appendix T, IBM Cloud Services Agreement For IBM Federal Data Centers. During the contract period, International Business Machines Corporation (IBM) and the Government agree that these terms and conditions will apply to any order for IBM Cloud Services.

The term "Government" shall mean all Federal agencies (as defined in Paragraph (b) of 40 USC 472) the Senate, the House of Representatives, the Architect of the Capitol, and the Government of the District of Columbia, all of which are hereinafter referred to as the Government. The services under this Special Item will be available to the Government within the United States, the District of Columbia and Puerto Rico. Such sales will be made to the Government within the United States, the District of Columbia and Puerto Rico. On a case-by-case basis IBM will perform Services to overseas U.S. Government locations which are in support of national defense operations (including U.S. Embassies), and to locations which support the national interest of the United States.

1. SCOPE

The prices, terms and conditions stated under Special Item Number (SIN) 132-40 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 Definition of Cloud Computing Essential Characteristics. Services relating to or impinging on cloud that do not meet all NIST essential characteristics should be listed in other SINs.

The scope of this SIN is limited to cloud capabilities provided entirely as a service. Hardware, software and other artifacts supporting the physical construction of a private or other cloud are out of scope for this SIN. Currently, an Ordering Activity can procure the hardware and software needed to build on premise cloud functionality, through combining different services on other IT Schedule 70 SINs (e.g. 132-51).

Sub-categories in scope for this SIN are the three NIST Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Offerors may optionally select a single sub-category that best fits a proposed cloud service offering. Only one sub-category may be selected per each proposed cloud service offering. Offerors may elect to submit multiple cloud service offerings, each with its own single sub-category. The selection of one of three sub-categories does not prevent Offerors from competing for orders under the other two sub-categories.

See service model guidance for advice on sub-category selection.

Sub-category selection within this SIN is optional for any individual cloud service offering, and new cloud computing technologies that do not align with 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:

IBM's offering under this SIN includes Software as a Service and Infrastructure as a Service.

IBM's Softlayer IaaS offering is provided to government customers as a subscription service. It provides the capability for a Client to provision processing, storage, networks, and other fundamental computing resources upon which a Client can run an array of software, including operating systems and applications. IBM's Softlayer Federal Cloud (SFC) has specific data centers for government customers that meets FISMA and FedRamp requirements.

● Commercially available cloud computing services ● Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing essential characteristics ● 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 platform or infrastructure. Limited application level configuration may be available. 2. **Platform as a Service (PaaS):** Consumer deploys applications onto cloud platform service using provider-supplied tools. Has control over deployed applications and some limited platform configuration but does not manage the platform or infrastructure. 3. **Infrastructure as a Service (IaaS):** Consumer provisions computing resources. Has control over OS, storage, platform, deployed applications and some limited infrastructure configuration, but does not manage the infrastructure.

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. Acceptance Testing

Any required Acceptance Test Plans and Procedures shall be negotiated by the Ordering Activity at task order level. The Contractor shall perform acceptance testing of the systems for Ordering Activity based on mutually agreed to and approved test procedures.

b. Training

Training, if requested shall be performed under SIN 132-51, Services.

c. Information Assurance/Security Requirements

IBM's information assurance/security requirements are in accordance with the SFC terms outlined herein and within Appendix T.

d. Related Professional Services

The Contractor is responsible for working with the Ordering Activity to identify related professional

services and any other services available on other SINs that may be associated with deploying a complete cloud solution. Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN and available under SIN 132-51.

e. Performance of Cloud Computing Services

The Contractor shall respond to Ordering Activity requirements at the Task Order level. Responses will be based on requirements outlined in the Request for Proposal. Contractors may include 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.

f. Reporting

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.

4. RESPONSIBILITIES OF THE ORDERING ACTIVITY

The Ordering Activity is responsible for indicating the cloud computing services requirements unique to the Ordering Activity. Additional requirements 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.

Cloud services typically operate under a shared responsibility model, with some responsibilities assigned to the Cloud Service Provider (CSP), some assigned to the Ordering Activity, and others shared between the two. The distribution of responsibilities will vary between providers and across service models. Ordering activities should engage with CSPs to fully understand and evaluate the shared responsibility model proposed. Federal Risk and Authorization Management Program (FedRAMP) documentation will be helpful regarding the security aspects of shared responsibilities, but operational aspects may require additional discussion with the provider.

a. Ordering Activity Information Assurance/Security Requirements Guidance

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 for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work.[2] The Contractor 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.

---

2 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*"**)

iv. The Ordering Activity has final responsibility 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. A memorandum issued by the Office of Management and Budget (OMB) on Dec 8, 2011 outlines the responsibilities of Executive departments and agencies in the context of FedRAMP compliance. [3]

v. Ordering activities are responsible for determining any additional information assurance and security related requirements based on the nature of the application and relevant mandates.

b. Deployment Model

If a particular deployment model (Private, Public, Community, or Hybrid) is desired, Ordering Activities are responsible for identifying the desired model(s). Alternately, Ordering Activities could identify requirements and assess Contractor responses to determine the most appropriate deployment model(s).

c. 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.*

d. Interoperability

Ordering Activities are responsible for identifying interoperability requirements. Ordering Activities should clearly delineate requirements for API implementation and standards conformance.

e. 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.

f. Reporting

The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of the initial requirement.

g. Privacy

The Ordering Activity should specify the privacy characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could be requiring assurance that the service is capable of safeguarding Personally Identifiable Information (PII), in accordance with NIST SP 800-122[4] and OMB memos M-06-16[5] and M-

---

3 MEMORANDUM FOR CHIEF INFORMATION OFFICERS: Security Authorization of Information Systems in Cloud Computing Environments. December 8, 2011.

4 **NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"**

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

07-16[6]. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy.

h. Accessibility

The Ordering Activity should specify the accessibility characteristics of their service and engage with the Contractor to determine the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could require assurance that the service is capable of providing accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

i. Geographic Requirements

Ordering activities are responsible for specifying any geographic requirements and engaging with the Contractor to determine that the cloud services offered have the capabilities to meet geographic requirements for all anticipated task orders. Common geographic concerns could include whether service data, processes and related artifacts can be confined on request to the United States and its territories, or the continental United States (CONUS).

j. Data Ownership and Retrieval and Intellectual Property

Intellectual property rights are not typically transferred in a cloud model. In general, CSPs retain ownership of the Intellectual Property (IP) underlying their services and the customer retains ownership of its intellectual property. The CSP gives the customer a license to use the cloud services for the duration of the contract without transferring rights. The government retains ownership of the IP and data they bring to the customized use of the service as spelled out in the FAR and related materials.

General considerations of data ownership and retrieval are covered under the terms of Schedule 70 and the FAR and other laws, ordinances, and regulations (Federal, State, City, or otherwise). Because of considerations arising from cloud shared responsibility models, ordering activities should engage with the Contractor to develop more cloud-specific understandings of the boundaries between data owned by the government and that owned by the cloud service provider, and the specific terms of data retrieval.

In all cases, the Ordering Activity should enter into an agreement with a clear and enforceable understanding of the boundaries between government and cloud service provider data, and the form, format and mode of delivery for each kind of data belonging to the government.

The Ordering Activity should expect that the Contractor shall transfer data to the government at the government's request at any time, and in all cases when the service or order is terminated for any reason, by means, in formats and within a scope clearly understood at the initiation of the service Example cases that might require clarification include status and mode of delivery for:

- Configuration information created by the government and affecting the government's use of the cloud provider's service.
- Virtual machine configurations created by the government but operating on the cloud provider's service.

---

[6] **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

- Profile, configuration and other metadata used to configure SaaS application services or PaaS platform services.

The key is to determine in advance the ownership of classes of data and the means by which Government owned data can be returned to the Government.

k. Service Location Distribution

The Ordering Activity should determine requirements for continuity of operations and performance and engage with the Contractor to ensure that cloud services have adequate service location distribution to meet anticipated requirements. Typical concerns include ensuring that:

- Physical locations underlying the cloud are numerous enough to provide continuity of operations and geographically separate enough to avoid an anticipated single point of failure within the scope of anticipated emergency events.
- Service endpoints for the cloud are able to meet anticipated performance requirements in terms of geographic proximity to service requestors.

Note that cloud providers may address concerns in the form of minimum distance between service locations, general regions where service locations are available, etc.

l. Related Professional Services

Ordering activities should engage with Contractors to discuss the availability of limited assistance with initial setup, training and access to the services that may be available through this SIN.

Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN. Ordering activities should consult the appropriate GSA professional services schedule.

m. IBM's Softlayer Federal Cloud (IaaS) Service Description terms (see section below Additional IBM Terms and Conditions) outlines terms and conditions relative to the management and responsibility of the Government for its data/content in the IBM SFC datacenter.

5. GUIDANCE FOR CONTRACTORS

This section offers guidance for interpreting the Contractor Description Requirements in Table 2, including the NIST essential cloud characteristics, service models and deployment models. This section is not a list of requirements.

Contractor-specific definitions of cloud computing characteristics and models or significant variances from the NIST essential characteristics or models are discouraged and will **not** be considered in the scope of this SIN or accepted in response to Factors for Evaluation. The only applicable cloud characteristics, service model/subcategories and deployment models for this SIN will be drawn from the NIST 800-145 special publication. 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[7].

Contractors must select deployment models corresponding to each way the service can be deployed. Multiple deployment model designations for a single cloud service are permitted but at least one deployment model must be selected.

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

In addition, 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.

Both service and deployment model designations must accord with NIST definitions. Guidance is offered in this document on making the most appropriate selection.

a. NIST Essential Characteristics

General Guidance

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 government entities cannot always leverage a cloud service to the extent that all NIST essential characteristics are commercially available. For the purposes of the Cloud SIN, meeting the NIST essential characteristics is determined by whether each essential capability of the commercial service is available for the service, 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 the Contractor should interpret the characteristics in light of current government contracting processes.

Table 3: Guidance on Meeting NIST Essential Characteristics

Characteristic	Capability	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 may approach on-demand in a variety of ways, including "not-to-exceed" limits, or imposing monthly or annual payments on what are essentially on demand services. 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 at the task order level: • 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	Ordering activities	Broad network access must be available without

Characteristic	Capability	Guidance
Access	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	significant qualification and in relation to the deployment model and security domain of the service • Contractors must specify any ancillary activities, services or equipment required to access cloud services or integrate cloud with other cloud or non-cloud networks and 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 Contractor • Resources may have general characteristics such as regional location	• The cloud service must draw from a pool of resources and provide 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 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 to access a private cloud deployment service. However the provisioned cloud 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. via a console operation or programming interface call, are required.

Characteristic	Capability	Guidance
	• 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

Inheriting Essential Characteristics

Cloud services may depend on other cloud services, and cloud service models such as PaaS and SaaS are able to inherit essential characteristics from other cloud services that support them. For example a PaaS platform service can inherit the broad network access made available by the IaaS service it runs on, and in such a situation would be fully compliant with the broad network access essential characteristic. Services inheriting essential characteristics must make the inherited characteristic fully available at their level of delivery to claim the relevant characteristic by inheritance.

Inheriting characteristics does not require the inheriting provider to directly bundle or integrate the inherited service, but it does require a reasonable measure of support and identification. For example, the Ordering Activity may acquire an IaaS service from "Provider A" and a PaaS service from "Provider B". The PaaS service may inherit broad network access from "Provider A" but must identify and support the inherited service as an acceptable IaaS provider.

Assessing Broad Network Access

Typically broad network access for public deployment models implies high bandwidth access from the public internet for authorized users. In a private cloud deployment internet access might be considered broad access, as might be access through a dedicated shared high bandwidth network connection from the Ordering Activity, in accord with the private nature of the deployment model.

Resource Pooling and Private Cloud

All cloud resource pools are finite, and only give the appearance of infinite resources when sufficiently large, as is sometimes the case with a public cloud. The resource pool supporting a private cloud is typically smaller with more visible limits. A finite pool of resources purchased as a private cloud service qualifies as resource pooling so long as the resources within the pool can be dynamically allocated to the ultimate users of the resource, even though the pool itself appears finite to the Ordering Activity that procures access to the pool as a source of dynamic service allocation.

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 commercially marketed 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 commercially marketed 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 commercially marketed 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 appropriate descriptions (include commercial marketing terms) 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**. 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, along 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. Alternatively contractors may choose to submit multiple service offerings for the SIN, each optionally and separately subcategorized.

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 provisioning then configuration, equivalent to procuring and then 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	Select a PaaS model for service based equivalents of complete or partial software

Service Model	Guidance
Service (PaaS)	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. • A limited range of configuration options for the platform service may be available. 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 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

Service Model	Guidance
	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 application services the SaaS service 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 non-cloud 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.

c. 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, but 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 the Contractor should interpret the deployment model characteristics. Contractors should take care to select the range of NIST deployment models most closely corresponding to each service offered.

Note that the scope of this SIN does not include hardware or software components used to construct a cloud, only cloud capabilities delivered as a service, as noted in the Scope section.

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.

Additional IBM Terms and Conditions

IBM Software as a Service (SaaS Offering)

1. IBM's Software As A Service Offering (SaaS)

The applicable terms for IBM's SaaS offering include Appendix T (Cloud Services Agreement for US Federal Government Clients), the US Government Supplement to the specific SaaS offering and the specific SaaS offering Service Description Document. The US Government Supplement and Service Description documents

can be found at the following website (see the US Gov't tab) http://www-03.ibm.com/software/sla/sladb.nsf/sla/usg

IBM Softlayer Federal Cloud (SFC) IaaS Offering

Service Description

This Service Description describes the Cloud Service IBM makes available to Clients under the Federal Cloud Service Agreement, Appendix T (or equivalent Cloud Service terms between the parties)(Agreement).

The Softlayer Federal Cloud Service Description document is provided as a separate attachment to Chapter 10.