**Special Item Number 518210C - Cloud and Cloud-Related IT Professional Services**

**Specific Information for Offerors**

**Table 1: Cloud Computing Services (i.e. IaaS, etc.)**

|  |  |
| --- | --- |
| SIN Description | Sub-Categories |
| ● 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. |

**NOTE: Offerors may optionally select the single sub-category that best fits each cloud service offering, per Service Model Guidance, or select no sub-category if the offering does not fit an existing NIST service model.**

1. **DESCRIPTION OF CLOUD COMPUTING SERVICES (i.e. IaaS, etc.) AND PRICING**
2. The information provided below is designed to assist Offerors in qualifying cloud computing services and provide complete descriptions.
3. In addition to standard pricing requirements, 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.

Table 2 summarizes the additional Offeror provided description requirements for services proposed under the Cloud Computing Services (i.e IaaS, etc.). All mandatory description requirements must be complete, and adequate according to evaluation criteria.

In addition there is one “Optional” reporting descriptions which exists to provide convenient service selection by relevant criteria. Where provided, optional description requirements must be complete and adequate according to evaluation criteria:

1. The NIST Service Model provides 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 the specific service offering.
2. If a sub-category is selected it will be evaluated with respect to the NIST Service Model definitions and guidelines in “Guidance for Contractors".

**Table 2: Cloud Service Description Requirements**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Description Requirement** | **Reporting Type** | **Instructions** |
| 1 | Provide a brief written description of how the proposed cloud computing services (i.e. IaaS, etc.) satisfies each individual essential NIST Characteristic | Mandatory | The cloud service must be capable of satisfying each of the five NIST essential Characteristics as outlined in NIST Special Publication 800-145. See ‘GUIDANCE FOR CONTRACTORS: NIST Essential Characteristics’ below in this document for detailed overall direction, as well as guidance on inheriting essential characteristics. The NIST “Measured Service” characteristic requires a minimal “pay as you go” unit of measurement appropriate for the service. In the case of SaaS, the appropriate maximum measured increment of service shall be no more than 30 days per user, or some other equivalent discrete measurement that provides the government with the advantage of frequent (approximately every 30 days) “pay as you go” metering cycles. SaaS products, where consumption is only measured on an annual basis, may better fit under “Term Software License” SIN 132-32. Likewise, offers of any combinations of IaaS, PaaS or any other cloud product services in a bundle or other fashion that do not meet the frequency requirements of approximately 30-day measurement and billing cycles, will not be accepted as complying with the NIST Measured Service characteristic. |
| 2 | Select NIST deployment models for the cloud computing service proposed. | Mandatory | Contractors must select at least one NIST deployment model as outlined in NIST Special Publication 800- 145 describing how the proposed cloud computing service is deployed. Select multiple deployment models if the service is offered in more than one deployment model.  See ‘GUIDANCE FOR CONTRACTORS: NIST Deployment Model’ below in this document for detailed direction on how to best categorize a service for the NIST deployment models. |
| 3 | 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 as outlined in NIST Special Publication 800-145. Sub-category selection is optional but recommended. See ‘GUIDANCE FOR CONTRACTORS: NIST Service Model’ below in this document for detailed direction on how to best categorize a service for the NIST IaaS, PaaS, and SaaS service models. |

1. **GUIDANCE FOR OFFERORS**

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

Offeror 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 evaluation factors. 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 (i.e. IaaS, etc.) under this SIN must substantially satisfy the essential characteristics of cloud computing as documented in the NIST Definition of Cloud Computing [SP 800-145](http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)[[1]](#footnote-1)

Offerors 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.

Both Cloud service model (i.e. IaaS, etc.) and deployment model (i.e. public, etc.) designations must accord with NIST definitions. Guidance is offered in this document on making the most appropriate selection

* 1. 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 other appropriate payment cycles 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 Access | ● Ordering activities are able to access services over standard agency networks  ● Service can be accessed and provisionedusing standard devices such as browsers, tablets and mobile phones | ● Broad network access must be available without 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 simple 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  ● ‘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.  ● 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  ● The goal of the Measured Service requirement is to ensure Ordering Activities realize the full benefit of “pay as you go” consumption models. Consumption measurements that are not discrete enough or frequent enough (greater than 30 days), will not fulfill this NIST essential characteristic and will not be eligible for inclusion in this SIN. |

|  |
| --- |
| **Inheriting Essential Characteristics** |

Cloud Services (i.e. IaaS, etc.) 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. Cloud Services (i.e. IaaS, etc.) 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.

1. 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 Cloud services (i.e. IaaS, etc.) 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 (including 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 Cloud Service (i.e. IaaS, etc.). 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 4 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 4: 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 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.  ● 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 a 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 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 gray 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. |

1. 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 5: 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. |

1. **7** [**http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf**](http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf) [↑](#footnote-ref-1)