Infrastructure as a Service (IaaS)

Infrastructure as a Service is one of four EIS cloud services. It provides an agency with a secure, cloud-based IT environment with all of the typical components such as computers, servers, network storage, etc. IaaS consists of two sub-services:

- **Private Cloud:** Provides a secure, segregated IT environment for an agency. It includes virtual machines, storage, server hosting, security components, storage backup, continuity of operation and disaster recovery services. The cloud platform provides the necessary network infrastructure such as LANs, load balancers and firewalls.

- **Data Center Augmentation with Common IT Service Management (ITSM):** Enables augmentation of already virtualized agency premises data center resources with dynamically expandable and contractible virtualized cloud-based resources that also includes a common IT management framework for agency data center resources and cloud resources.

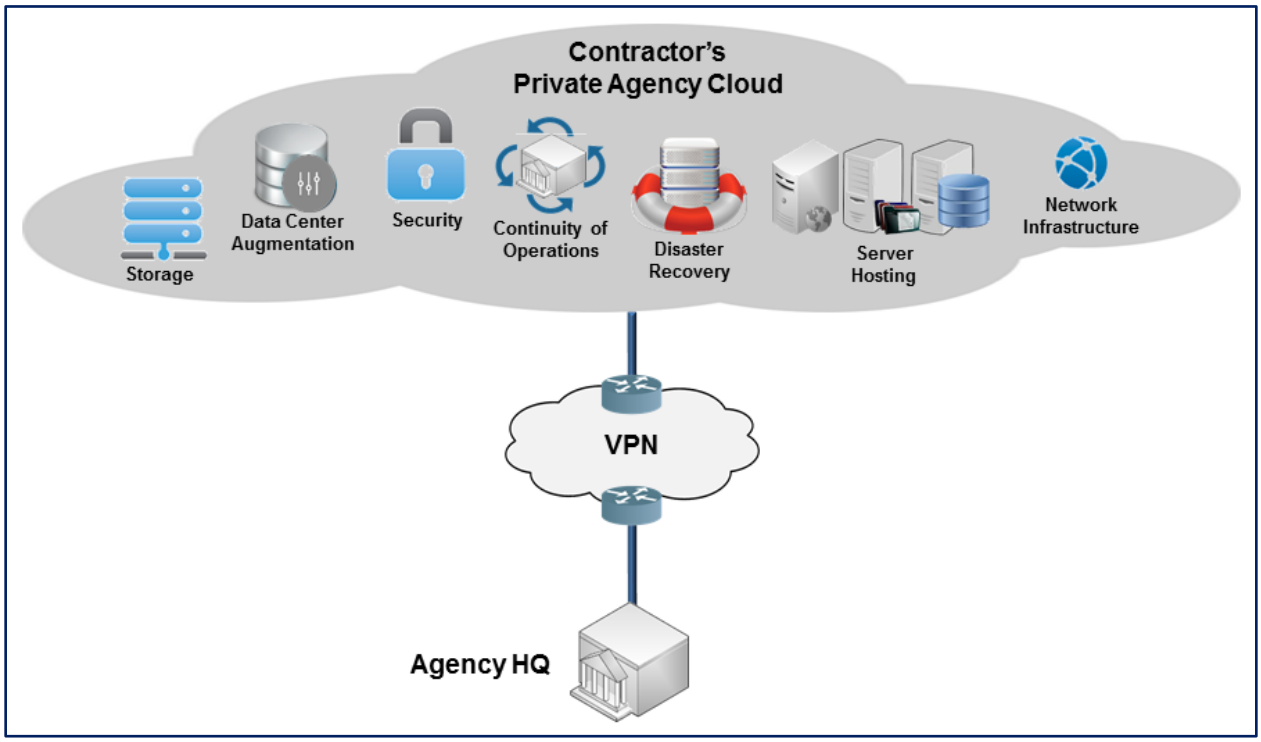
IaaS meets all federally required security standards for Cloud services supporting requirements for the FedRAMP and Trusted Internet Connection (TIC), a technology designed to provide fast and secure computing for mobile federal personnel.

Category: Cloud Services

Complementary Services Needed: In order to use IaaS, the agency may need one or more of the following EIS services or equivalents: Access Arrangements (AAs) or Virtual Private Network Service (VPNS).

Definitions: Please see EIS contract Section J.12 Glossary of Terms for clarification of technical terms and acronyms.

Figure 1–Infrastructure as a Service Diagram



1. Why an Agency Might Select this Service

- Reduces hardware and infrastructure expenses. The IaaS cloud platform provides the necessary network infrastructure (e.g., LAN, load balancer, and firewall), security components, and storage backup services.
- Reduces IT staff and administration costs.
- Reduces the risk and expense of testing and adopting new technologies.
- IaaS dynamic scalability simplifies capacity planning and can lower capacity costs.

NOTE: Agencies considering this service may also want to compare it with Software as a Service (SaaS) and Platform as a Service (PaaS).

2. Examples of How IaaS Could be Used

- **Entire Infrastructure Hosting:** An agency could reduce the risk and expense of maintaining its own IT infrastructure by having the IaaS contractor host most of the agency's hardware, software, user applications, servers and storage.
- **Dynamic Resource Allocation:** An agency that experiences peaks and lows on its public facing websites could use the service's automatic capacity features to dynamically expand and contract resources as needed. This could help reduce the expense and complexity of managing the workloads, and ensure an improved user experience.
- **Disaster Recovery (DR) and Continuity of Operations (COOP):** An agency could take advantage of the consolidated and streamlined DR and COOP functions that IaaS provides to reduce DR and COOP costs, simplify related planning and improve the ablity of the agency to survive a disaster.
- **Federal Geospatial Data Clearinghouse (FGDC) Example:** The FGDC's GeoCloud Initiative used IaaS capabilities to deploy services and solutions to improve public access to geospatial data beyond in-house capabilities. The solution increased speed of response, reliability, failover and security. It also provides better handling of peak load situations.

3. Key Technical Specifications

NOTE: This portion of the service guide has been abridged due to space considerations. For full technical details on IaaS, please refer to EIS contract Section C.2.5.1.

Table 1—Technical Capabilities of Private Cloud IaaS

Capability	*Description*
Access to Agency Data in Data Centers	Complies with National Policy as defined in C.1.8.8 including agency sites and remote locations.
Cloud Data Center Security	a) Provide secure connectivity among service provider's data centers for elasticity (expansion and contraction) of computing resources. b) Secure connectivity to service provider's data center from agency sites. c) Provide additional compliance and certification requirements as specified in the TO.
Agency Cloud Service Security	a) Create and maintain a security perimeter around an agency's data and VMs. b) Data-at-rest encryption in accordance with FIPS 197.
Virtualized Elastic Computing Infrastructure	a) Virtual Machines (VMs) b) Network Storage
Server Hosting	a) Private-facing Internal Web Hosting b) Public-facing External Web Hosting
Backup and Restore	Backup and Restore agency data.
On-Demand Self-Service	On-demand self-service of IaaS provisioning, configuration management, topology management, security management, activation and deactivation via portal scripting language or API with role based access control for portal login which is OMB M-11-11 compliant.
Measured/Metered Usage Visibility	Visibility into usage of measured/metered (usage-based) service.
Virtual Machine with Private IP Address Blocks	Allow users to have VMs with their own private IP address blocks.
Virtual Machine Bulk Import/Export	Support bulk import and export of VM per ISO 17203.
User Access to Log Events	Allow users access to log events such as resource provisioning and de-provisioning, VM start and stop, and account changes, for at least 60 days.
Metadata Tags with Run Reports (NOTE: May not be available from all contractors.)	Allow users to place metadata tags on provisioned resources and to run reports based on them, which is useful for internal showback or chargeback.
Cost Control Measures and Leases	Support cost control measures such as quotas (limits on what a user can provision) and leases (time-limited provisioning of resources).

Capability	*Description*
24x7 Customer Service	Support with 24x7 customer service, via phone, email and chat.
Cloud Data Ownership	Agency retains exclusive ownership over all of its data in the cloud. The contractor provides tools to allow the client agency to fully retrieve its data in the original or a mutually agreed-upon format.
Cloud Resources Location	Cloud resources, particularly the data at rest, must be located within the U.S. or the jurisdiction identified in the TO to allow electronic discovery (eDiscovery) of identification, collection, processing, forensic analysis, auditing, and production of Electronically Stored Information (ESI) required in the discovery phase of litigation. (Please see EIS contract Section H.33 E-Discovery for Cloud-Based Services for more details on eDiscovery requirements.)
Disaster Recovery and Continuity of Operations	Provides Disaster Recovery (DR) and Continuity of Operations (COOP) per agency-specific requirements in the TO.

Table 2—Technical Capabilities of Data Center Augmentation with Common ITSM

Capability	*Description*
Cloud and Data Center Virtual Resource Management	Ability to manage both cloud virtual resources and the agency data center's virtual resources with interoperable monitoring and control capabilities.
Management Platform	Management platform includes a visual indicator of which resources are in the cloud and which are premises resources.
Data Center Management Platform Integration (NOTE: May not be available from all contractors.)	Ability to integrate with agency's data center management platform.

Table 3—IaaS Features

Feature	*Description*
"Bare Metal" Physical Servers **(NOTE: May not be available from all contractors.)**	Ability to have "bare metal" physical servers on a dynamic basis with provisioning times of two hours or less. This capability may be required for (a) a large-scale database requiring an incremental storage capacity, or (b) specialized network equipment that may not be available in the cloud, or (c) software that cannot be licensed on virtualized servers, or (d) legacy equipment that cannot be virtualized, or (e) agencies that plan to move into collocation first and then gradually migrate into the provider's cloud.
Data Management and Analytics	Capability complements and extends log management and analysis services and other data center management services, per agency-specific requirements in the task order (TO).

4. Pricing Basics for IaaS

NOTE: IaaS is a catalog-priced service.

Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide to gain an understanding of EIS pricing fundamentals.

4.1 Access Arrangements

Appropriate access arrangements must be selected for each endpoint. Please visit the EIS Resources Listing and locate the Access Arrangements Guide for more detailed information.

4.2 Service Related Equipment (SRE)

- SRE must be chosen based on equipment required at each location. NOTE: SRE uses Catalog-based Pricing.
- Request that contractor provide pricing for any SRE that would be required, in addition to the agency's existing infrastructure, to deliver the service.
- Please visit the EIS Resources Listing and locate the Service Related Equipment Service Guide for more detailed information.

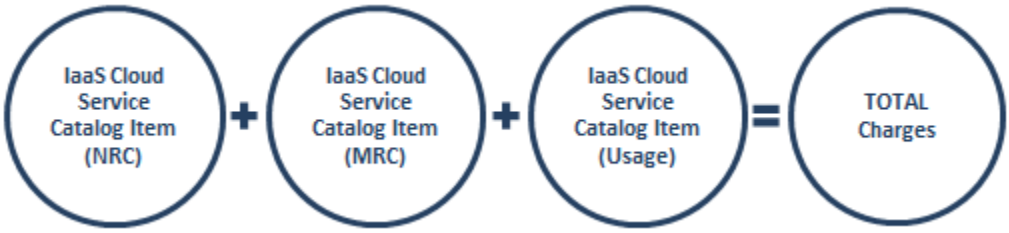
4.3 IaaS Price Components

The price structure for IaaS consists of the components shown in *Table 4* below.

Table 4—IaaS Pricing Components

Component	*Charging Unit*
IaaS Cloud Service Catalog Item (NRC)	ICB
IaaS Cloud Service Catalog Item (MRC)	ICB
IaaS Cloud Service Catalog Item (Usage)	ICB

Figure 2—This figure shows how the various pricing components in Table 4 would be combined to calculate the total IaaS charges. NOTE: One or more of these components may not be needed to price a particular service package



NOTE: A contractor may offer a custom variation of the service to meet an agency's unique requirements. Such a customization would be identified with a Task Order Unique CLIN (TUC), and would include charges that would have to be added to the components in *Figure 2* to determine the total cost of the service.

4.4 IaaS Pricing Examples

NOTE: IaaS is a Catalog-based Service. No pricing examples are provided, as the specific services available vary based on each contractor's cloud service catalog.

For a general example of pricing a Catalog-based Service, please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide, and, in particular, the Guide's Section 6 on Catalog-based Pricing.

5. References and Other Sources of Information

- For more details and information on IaaS technical specifications and requirements, please refer to EIS contract Section C.2.5.1; for pricing details, please refer to Section B.2.5.
- For more information on service-related items, please see:
    - EIS contract Section B.2.10 Service Related Equipment
    - EIS contract Section B.2.11 Service Related Labor
- Please refer to a contractor's individual EIS contract for specifics on the contractor's IaaS offerings.
- For additional EIS information and tools, visit the EIS Resources Listing.
- For guidance on transitioning to EIS, please visit EIS Transition Training where you'll find several brief video training modules.