UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE CHIEF INFORMATION OFFICER

CLOUD STRATEGY

Version 1.3

OFFICE OF CHIEF INFORMATION OFFICER (OCIO)
1900 E. ST. NW
Washington, DC 20415

July 2012

Revision History

Version	Date	Summary
1.1	November 2011	Initial Draft
1.2	April 2012	Final Version
1.3	July 2012	Revised Final

Approved ______________________ Date 07/26/2012

MATTHEW E. PERRY, CIO, OPM

Table of Contents

1. Background and Description

After an analysis of the U.S. Office of Personnel Management's (OPM) key business drivers for maturing the IT infrastructure towards a cloud model; OPM OCIO has initiated an effort to identify applications that can be Cloud enabled and to aggressively adopt Cloud computing across the Agency.

Cloud computing is defined by the Computer Security Division, Information Technology Laboratory, National Institutes of Standards and Technology[1] as:

> *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

Cloud Computing is a significant computing trend with the potential to greatly improve IT agility while reducing overall IT cost. It is an evolving term that describes the development of many existing technologies into end-user consumable services. Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of computing resources. These components can be rapidly provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption. In the current computing environment, business and system owners typically pay for the resources being used, but also all the extra computing power that is simply waiting to be used if/when it is needed. By leveraging the Cloud model on the other hand, the business owners now have the ability to only pay for the computing power that they actually use which frees up those extra funds for other key initiatives.

Adopting Cloud computing is a complex decision involving many factors. It is OPM OCIO's objective to develop, document and implement a framework to discern the optimal computing configuration for specific applications and highlight the key differentiators that will enable Agency business leaders to make informed decisions, improve their customers' experience, and leverage the cost saving benefits.

It is important to note, that while the terminology of Cloud based computing might be relatively recent, OPM has developed and maintained computing platforms that service the entire Federal government for many years. These systems such as USAJobs, USAStaffing, and eQIP provide human resource and investigative services to the Federal government as a whole These centralized systems, provided to the entire federal government,are in line with our agency's core competency, therefore allowing other agency's to use our expertise and not fund their own systems therefore providing efficient use of Federal IT expenditures.   OPM continues to evaluate all new IT solutions, including Federal wide offerings for relevance to the cloud.

[1] NIST Special Publication 800-145, The NIST Definition of Cloud Computing, Page 6

This document focuses on identification of specific approaches and strategies for OPM to adopt Cloud computing. OPM OCIO has identified the workload attributes and requirements to access workload applicability for Cloud computing. The OPM OCIO Cloud strategy presented in this document is based not only on the industry research but also draws on our experiences creating Private Cloud offerings. Specifically our experience with USAJobs and other Cloud efforts have successfully demonstrated the technology capabilities and have substantiated the business drivers listed in this document.

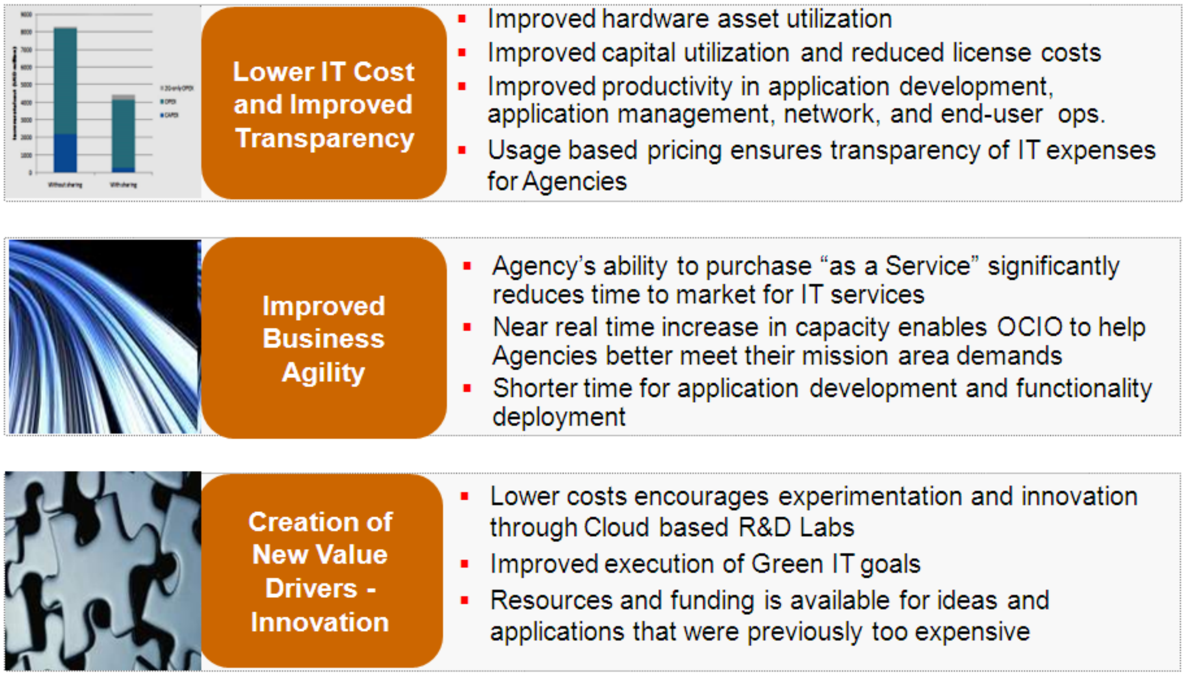
2. Cloud Business Drivers

Cloud Computing will enable OPM to respond more effectively to the changing business needs and provide agency users access to incremental computing resources at significantly lower cost. This new computing service model will yield tremendous advantages for agency users, especially those with applications that support dynamic workloads. OPM OCIO has identified three key drivers for Cloud computing adoption across OPM agencies:

- Lower IT cost and improved transparency
- Improved business agility
- Innovation and creation of new value drivers

Figure 1 (shown below), expands on OPM's three key drivers for Cloud computing adoption and outlines several detailed benefits specific to OPM's current IT infrastructure. By leveraging these benefits, OPM OCIO can develop the "as-a-service" platform to provide more robust and less expensive IT services to OPM as a whole as well as other Federal Agencies.

Figure 1. Cloud Business Drivers for OPM



Lower IT Cost and Improved Transparency

- Improved hardware asset utilization
- Improved capital utilization and reduced license costs
- Improved productivity in application development, application management, network, and end-user ops.
- Usage based pricing ensures transparency of IT expenses for Agencies

Improved Business Agility

- Agency's ability to purchase "as a Service" significantly reduces time to market for IT services
- Near real time increase in capacity enables OCIO to help Agencies better meet their mission area demands
- Shorter time for application development and functionality deployment

Creation of New Value Drivers - Innovation

- Lower costs encourages experimentation and innovation through Cloud based R&D Labs
- Improved execution of Green IT goals
- Resources and funding is available for ideas and applications that were previously too expensive

2.1. Lower IT Cost and improved Transparency - Efficiency

OPM currently operates under well-defined signature authorities that dictate the values that the CIO is able to procure without additional approvals. The Cloud initiative will shift the spending at OPM from CAPEX to OPEX. It is probable the currently prescribed OPEX signature authority for the CIO is insufficient to support cloud operations. The Cloud computing value proposition enables OPM IT service providers to present a clear and more transparent pricing model based on the resource consumption for OPM programs. It will allow the IT program owners and customer agencies to ramp up their investment over time based on the consumption demand by the programs. This will free up funds for additional initiatives and greatly lower the historically large procurements needed for new applications/systems or technical refresh cycles.

The current model used for reviewing technology is fragmented between the Network Management, Data Center, and shadow IT. Each area has its own method for determining the technology required to fulfill the customer needs. This leads to duplication of efforts, limited standards acceptance / use, and other outcomes that are not conducive to efficient and agile IT operations.

By establishing a CIO-level technology review committee, decisions can be made based on a holistic view of the overall needs of IT and OPM. This will lead to greater user satisfaction, lower agency IT spend, technology convergence, tighter security and a common management model. Furthermore, by ensuring all new systems, applications and/or IT investments follow CIO-issued guidelines, OPM will be better positioned to leverage CIO and non-CIO funding to build and enhance a standardized and scalable IT infrastructure.

This review committee would not create any new organizational structures but would establish a group drawing from Enterprise Architecture, Network Management, Datacenter, Systems (Applications and Benefits) support and development organizations. This group would review any new requirements or significant changes to existing services. A cloud first model would be used during these evaluations. Overall, this committee would ensure that business owners would receive the greatest ROI for their IT-based procurements.

The Cloud Computing environment will reduce the need for capacity planning at an application/program level, which is a necessity in current IT investment models today. Agencies will be able to request IT resources on-demand from OPM; while OPM or its Cloud provider will make the investments to create effective demand management and capacity planning to ensure that the required computing power is available. The OPM infrastructure is in prime position to provide cloud services to other Government agencies. OPM is currently providing cloud services to Federal agencies through cloud services like USAJobs, USAStaffing and HR services. Potential OPM cloud offerings include desktop/server virtualization and storage.

Greater utilization of virtual farms for servers and storage will result in more optimal resource utilization and lower licensing cost. While OPM OCIO has several initiatives underway aimed at improving the utilization of infrastructure (e.g. Federal Data Center Consolidation - FDCC), Cloud computing will take these initiatives to the next level and will enable OPM to deliver the benefits of virtualization and shared workloads across the Agency.

2.2. Improved Business Agility

As identified in the OMB's Federal Cloud Computing Strategy, the impact of Cloud computing will be far more than economic. Cloud computing will allow agencies to improve services and respond to changing needs and regulations much more quickly. Cloud computing will also allow OPM agencies to rapidly scale up to meet unpredictable demand and minimize service disruptions. Furthermore, by leveraging Cloud computing methodologies, OPM can continue to reduce power consumption needs through continued standardization and modernization of a unified Cloud platform.

2.3. Creation of New Value Drivers - Innovation

Cloud computing will enable new generations of products and services to be introduced at a faster pace. Many business ideas or capabilities that require large amounts of computing power and scale that couldn't be implemented due to existing technical limitations or cost-effectiveness can now be realized. With fewer technical and economic barriers for provisioning IT services, Cloud Computing will enable prototyping and market validation of new ideas at a much faster pace and for significantly less upfront cost.

3. OPM Current Computing Environment

In 2011, the OPM infrastructure included 1577 servers running in four data centers with <50% virtualization. The computing servers were dedicated to specific applications, and each server was sized to support application growth and spikes in demand. As a result, OPM had low physical server utilization and limited ability to quickly provision new capacity. In addition, capacity planning to support new IT initiatives has been complicated by the need to manually gather configuration, historical purchasing, and other information.

Though this environment has met OPM's needs to date, the accelerating pace of business and budget cuts are driving a need to optimize the services and migrate away from physically dedicated infrastructures. These limitations made OPM one of the early adopters of virtualization among Federal Agencies. We started our Cloud journey like most large organizations – by first virtualizing the low end workloads and then in the next phase moving towards virtualization of high-end business applications. While not all large business applications are virtualized today at OPM, we are moving in that direction and are seeking greater asset utilization.

The wide breadth of technologies within OPM's IT infrastructure require continual review and analysis to provide the best virtualization options to leverage the inherent benefits of Cloud, while also providing a great user experience. A snapshot of the technologies that OPM supports includes Windows Server 2003 and 2008, Linux, UNIX, CentOS, Ubuntu, 3PAR, VMware, SQL Databases, and Oracle Databases. Some of these technologies assist in OPM's virtualization efforts, while others allow for easy virtualization, or in some cases pose challenges. OPM's OCIO will continue to study new Cloud-focused technologies in an effort to mitigate the remaining virtualization challenges while also maturing the overall IT infrastructure.

When considering which applications and systems may be moved to the Cloud, business owners must consider certain factors before proceeding. OPM has significant security, compliance and governance requirements. These requirements will need to be supported by potential cloud providers. The capabilities, agreed upon liabilities and responsibilities of each provider needs to be documented. Areas of consideration include:

- Pricing (e.g., pay-per-seat, pay-per-CPU hour)
- Performance (e.g., latency expectations, response time for storage IO)
- SLAs (e.g., Are the SLAs from the vendor equal to or better than OPM SLAs?)
- Support (e.g., U.S.-based, cleared support staff)
- Security (e.g., FISMA level)
- Vendor neutrality (e.g., only one operating system)
- Escape clause (e.g., How do I get my data out when the contract is done?)
- Backup / DR / COOP (e.g., vendor disaster recovery plans, Can I access my services from anywhere?)

- Data location (e.g., U.S.?, overseas?)
- Audit (e.g., vendor / customer / independent audits)
- Vendor vetting of potential customers (e.g., What information will OPM have to supply prior to becoming a customer?)

OPM's OCIO will be prepared to assist business owners in determining if the Cloud is right for them, as well as what flavor of Cloud is most suitable. Considerations must also be given to the type of information are stored within the applications and systems. OPM's mission and core business functions require the proper storage and use of PII data. This is a challenge that OPM must consider to ensure the security and auditability around the data. OPM applications / services that should immediately present issues with Public Cloud deployments include ones that:

- Deal with PII data;
- Require FISMA High; and/or
- Store or use classified data.

In these instances, only Private, Community or Government-only Hybrid cloud models should be considered. These options can be used to mitigate issues with PII through greater controls and monitoring capabilities that are inherent with those Cloud offerings.

OPM OCIO also conducted a Cloud Case Study focused on the OPM.gov website. The OCIO is committed to a cloud first strategy to ensure the most efficient use of IT resources and expenditures while providing flexible and scalable solutions in response to increased demand for IT. OPM had a need to upgrade the IT infrastructure supporting OPM.GOV web site and using a detailed cost benefit analysis in combination with the agency's cloud strategy, developed the most cost effective, feature rich solution set. In performing this assessment many often overlooked lifecycle costs were captured while comparing the desired features and capabilities which were compared between internal hosting capabilities and public cloud solutions. This return on investment exercise, identification of all lifecycle costs associated with the SDLC of an application, and the comparison of system feature requirements to public cloud readiness has been leveraged in additional application development efforts and provided lessons learned for OPM's Cloud Strategy implementation guide.

As a result of the cloud migration, OPM was able to increase the capabilities and support infrastructure of the OPM.Web system in a cost effective manner. Specifically, through using a Cloud solution provider, with burstable bandwidth and 24 x 7 support, OPM was able to avoid large capital expenditures for hardware, and additional costs for support staff. These savings equaled $1.4 M in the first year alone (the capital investment to host the site in house, plus the added support costs for 24x7 support compared to the cost of an alternative hosting solution. These realized cost savings and cost avoidance illustrates the strength of embracing a cloud approach to service providing. Through this exercise, the following lessons learned were documented:

- Changing perceptions, hearts and minds to have application developers move to a cloud cannot be under-estimated. This ‘box hugging’ mentality where they want to see their infrastructure takes a concerted effort to overcome
- Providing a technology agnostic approach and a robust evaluation matrix to evaluate solutions provides clarity and removes emotions from the evaluation process.
- Security concerns remain a significant driver and must be considered in the evaluation matrix
- Easy stand-alone web sites with limited dependencies to complex backed IT processes are a no brainer to move to the cloud. These web services are the focus of OPM initial Cloud migration implementation approach
- Systems that require burstable capabilities where investment in significant infrastructure to support increased processing capabilities for limited points in time (for instance open enrollment periods for services, or weather related status) are a prime candidate for the flexibility public clouds provide.

Leveraging what OPM learned to date through their Cloud readiness exercises and implementations, OPM will continue to mature their IT infrastructure through continual improvement processes and analysis of best of breed solutions. OPM OCIO will also use and update their existing ITSM processes to ensure a Cloud-first approach. An updated SDLC document is also being created to provide better IT Governance capabilities and provide further insight into what systems or applications are best positioned, or could benefit most from a migration to OPM’s Cloud infrastructure.

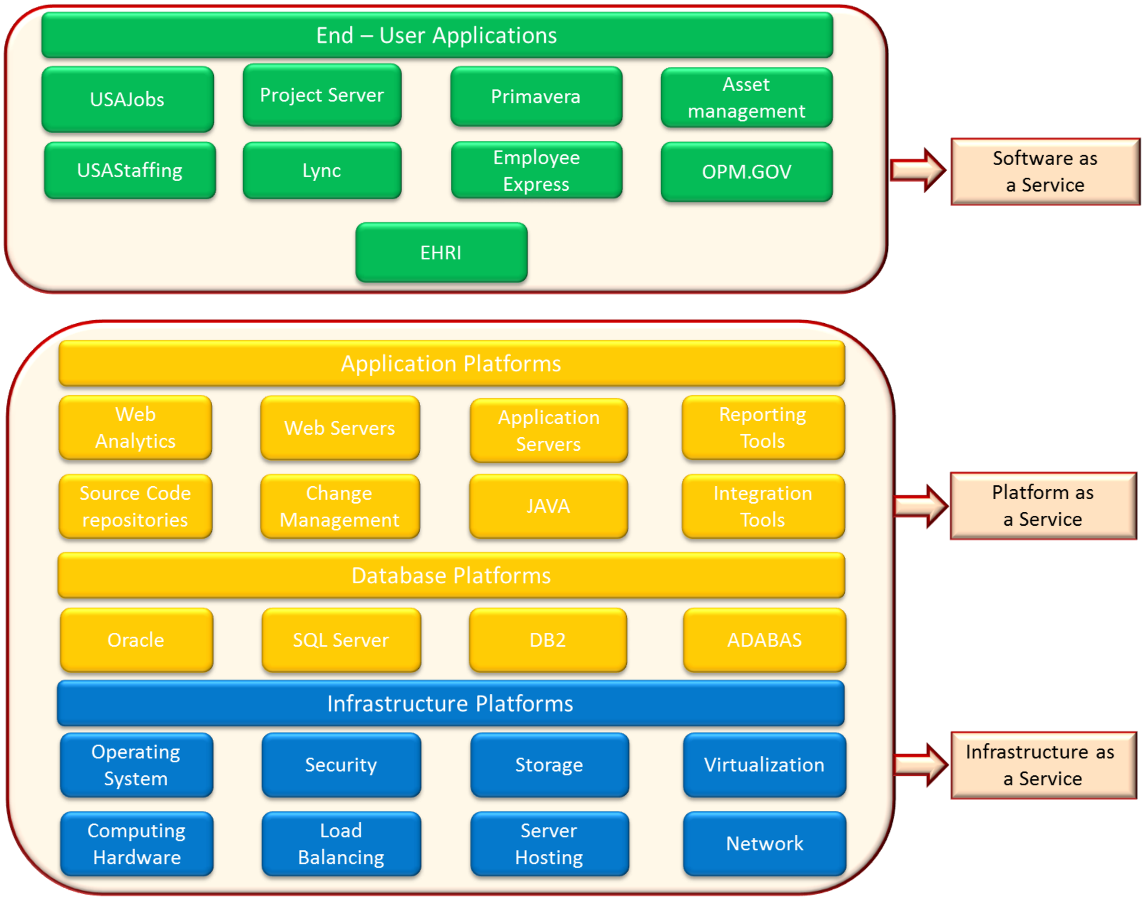
4. OPM Cloud Strategy – “Evolve On-demand Service Capabilities”

The OPM Cloud strategy is evolving from our current private Cloud offerings, federal data center consolidation (FDCC) and virtualization initiatives, which have already demonstrated that we can enhance our asset utilization and be significantly more agile.

The OPM OCIO vision is to dramatically optimize the delivery of all IT services by leveraging a combination of OPM Private Cloud and commercial vendor provided public Cloud capabilities and move towards a “IT-as-a-Service” paradigm. These comprehensive Cloud services will offer OPM agencies the flexibility of on-demand services and rapid elasticity while significantly reducing their IT investment through resource pooling.

The maturity of the Cloud computing business model and the Federal Data Center Consolidation efforts have presented OPM a unique opportunity to optimize the overall delivery of IT services. OPM private Cloud is a shared multi-tenant environment built to a highly efficient automated and virtualized infrastructure. Due to the extensive scope of this initiative, our strategy to deliver private Cloud capabilities will be based on Agency needs and will follow a phased approach over the next three years. As we add these capabilities, we expect that the Cloud will become capable of hosting highly demanding, mission-critical business applications.

Figure 2. OPM Cloud Vision – IT as a Service



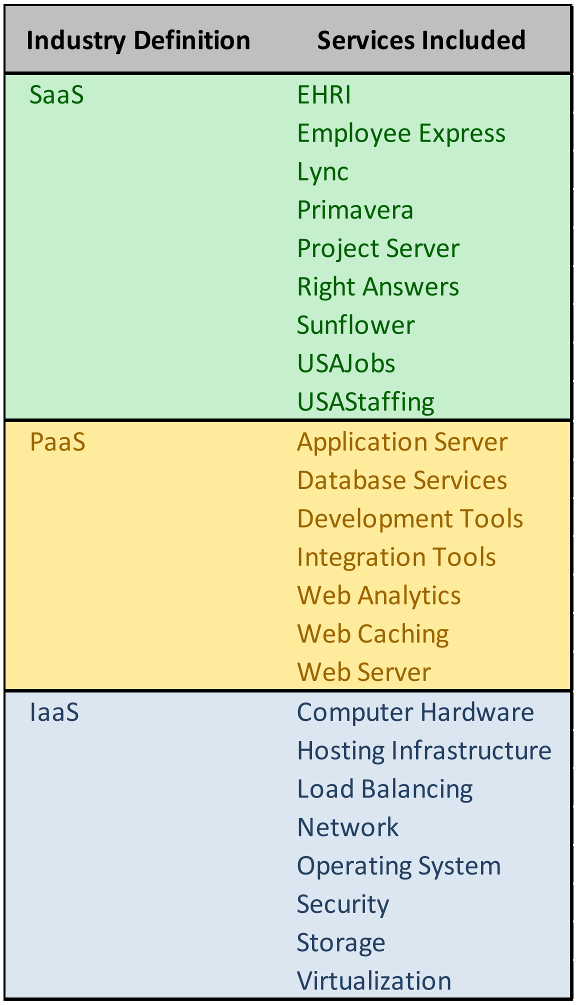
OPM's Private Cloud Strategy involves establishing robust Cloud infrastructure and offering a range of "Infrastructure as a Service" (IaaS) and "Platform as a Service" (PaaS) capabilities that meet OPM agencies' needs for secure, scalable, and cost effective IT solutions. OPM Private Cloud services will continue to evolve and offer greater flexibility and a larger number of pre-configured templates as required by customer agencies.

Given the discrete nature of IT projects, it is difficult to optimize the entire environment. OPM's approach will involve the development, documentation and implementation of re-usable service capabilities with predictable pricing to customer agencies so that they can leverage these capabilities/services "as-a-Service".

OPM will also incorporate the recently published FedRAMP guidelines for implementing a public Cloud. "The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services." FedRAMP's guidance will be a primary consideration in the continued maturation of the OPM Cloud initiative as components are added and new functionality is released. Once all FedRAMP controls and requirements are met, OPM will work with certified 3rd party assessors to receive the FedRAMP certification. This will better enable OPM to open up their Cloud offering to other agencies and government entities. Through a broader user base, OPM will also be better equip to provide higher quality services and more scalable solutions at a lower cost.

Figure 3 shows the target state of the "OPM - IT as a Service" vision, and the services that are currently available or planned as part of the private Cloud implementation. The IaaS section portrays OPM's goal to standardize on the hardware and other building blocks of the IT infrastructure (OS, virtual machines, storage, etc.). This will allow for greater ROI and buying power to build a robust infrastructure. The PaaS services support OPM's vision of a standard platform for all applications and systems to be built on. This will reduce fragmentation and the added costs inherent with supporting legacy or one-off systems. It will also provide a dynamic platform to increase resource allocation to the applications or services based on user demand. Finally, the SaaS section outlines services or applications that have been reviewed and deemed strong candidates for hosted applications and services. Some of the systems outlined are currently hosted at 3rd party data centers. By rolling these into OPM's Cloud infrastructure, the respective business owners would save significant costs associated with the current hosting and maintenance.

Figure 3. OPM “IT as a Service” – Current and Planned Services



Industry Definition	Services Included
SaaS	EHRI
	Employee Express
	Lync
	Primavera
	Project Server
	Right Answers
	Sunflower
	USAJobs
	USAStaffing
PaaS	Application Server
	Database Services
	Development Tools
	Integration Tools
	Web Analytics
	Web Caching
	Web Server
IaaS	Computer Hardware
	Hosting Infrastructure
	Load Balancing
	Network
	Operating System
	Security
	Storage
	Virtualization

4.1. IaaS Services

OPM started virtualization as a consolidation effort. The focus for OPM was on reducing capital expenses on server hardware, reducing energy costs and avoiding or delaying new data center or computer room build-outs. OPM plans on continued execution on the virtualization path to improve the services and offer operational improvements, flexibility, speed and ability to manage downtime more efficiently. We will introduce several value add capabilities like rapid provisioning and cloning of environments. These capabilities coupled with significant improvements to be made in measurement and chargeback approaches through the Enterprise Network Security Operations Center project will allow OPM to offer private Cloud services with Service Level Agreements across U.S. Federal Government agencies. With the right amount of capacity headroom for consumers, OPMs private Cloud implementation can convert OCIO from a source of limited resources to one that fosters innovation and efficiency — a huge benefit to agencies’ mission focus. Through a mature IaaS implementation, business, application or system owners no longer have to be concerned with procuring new hardware or IT components for a new initiative or tech refresh project. Instead, they can simply request the components and processing power they need, and have those requirements met with a Cloud provisioned platform at a fraction of the time and cost.

In order to build out a proper foundation for further Cloud strategies at OPM, it is critical that a standard baseline of hardware, software, storage and other necessary components are agreed on across functional groups and procurement offices. OPM OCIO has the following recommendations to achieve this vision:

- OCIO creates the IT Standard Baseline and obtains concurrent with Agency Groups
- OCIO reviews the components of the baseline quarterly to ensure they continue to strengthen the OPM Cloud platform
- All OPM Procurement offices validate that any IT purchases are in-line with the IT Standard Baseline
- OCIO Review Committee receive adequate notice of new IT purchases to provide a proper review and sign-off that the procurement is in line with OPM's Cloud-first Strategy

The Federal Government's CIO council also addresses the significant need to tackle the overall IT spend, the direction to do more with less, and the benefits of how Cloud can allow agencies to position themselves to pay only for the IT services they need rather than trying to account for the potential of max user loads. Below is an excerpt from the February 2012 CIO Council and Chief Acquisition Officers Council's joint publication, titled: *"Creating Effective Cloud Computing Contracts for the Federal Government – Best Practices for Acquiring IT as a Service":*

> *"The US Federal Government spends approximately $80 billion dollars on Information Technology (IT) annually. However, a significant portion of this spending goes towards maintaining aging and duplicative infrastructure. Instead of highly efficient IT assets enabling agencies to deliver mission services, much of this spending is characterized by low asset utilization, long lead times to acquire new services, and fragmented demand. To compound this problem, Federal agencies are being asked to do more with less while maintaining a high level of service to the American public.*
>
> *Cloud computing presents the Federal Government with an opportunity to transform its IT portfolio by giving agencies the ability to purchase a broad range of IT services in a utility- based model. This allows agencies to refocus their efforts on IT operational expenditures and only pay for IT services consumed instead of buying IT with a focus on capacity. Procuring IT services in a cloud computing model can help the Federal Government to increase operational efficiencies, resource utilization, and innovation across its IT portfolio, delivering a higher return on our investments to the American taxpayer."*

OPM currently offers several flavors of "Infrastructure as a Service" (IaaS) computing and storage services. The IaaS computing services offers pre-configured images of Linux, Windows and AIX operating systems deployed by OPM in a multitenant environment. It is an enterprise class offering allowing customers to deploy applications to highly resilient environments that offer high availability and performance that is comparable to the best in industry.

OPM IaaS will be offered using a shared infrastructure model that leverages virtualization capabilities that enable continuous, dynamic resource adjustments independent of physical placement of workloads. The shared, multitenant environment will allow OPM business owners to leverage the enterprise scale infrastructure without paying the high premium often associated with building a high-end infrastructure. The OPM IaaS platform will provide customers a high performance, secure operating environment with flexible sizing options to meet the needs of most customers. OPM IaaS computing services will be offered at 99.99% availability excluding scheduled downtime.

OPM Storage IaaS will include Storage Area Network (SAN) and/or Network Attached Storage (NAS) connectivity to different tiers of virtualized disk storage that vary in price and performance. OPM also will offer a fully managed backup and recovery service that utilizes standard network and SAN connectivity combined with centralized management software to provide point-in-time data protection of application data.

All IaaS services at OPM will be priced based on the usage and provide complete flexibility to the users to control their usage of resources.

FISMA Certified Commercial IaaS services will be made available to OPM agencies through a consolidated blanket purchase agreement (BPA) with leading commercial Cloud services providers. The objective of this offering is to provide OPM agencies with an option to use commercial hosting services for highly elastic workloads that may not fit into the OPM IaaS offering. The commercial IaaS will offer a full range of enterprise data center services to include secure, robust, and reliable application hosting and information services to meet present and future data center hosting requirements while ensuring OPM's ability to meet increasing computing and processing demands.

OPM's approach for acquiring FISMA certified commercial IaaS offerings are in line with the "Catalyzing Cloud Adoption" approach laid out in the Federal Cloud computing strategy. To improve readiness for OPM agencies Cloud computing adoption, the OCIO will facilitate an "approve once and use often" approach to streamline the approval process for Cloud service providers. Using the government-wide risk and authorization program for IaaS solutions, OPM will allow agencies to rely on existing authorizations so only additional, agency-specific requirements will need to be authorized separately.

4.2. PaaS Services

In accordance with the NIST definition, the OPM "Platform as a Service" (PaaS) services are defined as the capability provided to the consumer to deploy on the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. OPM plans to offer several PaaS services including database, application server, web server etc.

OPM PaaS-DB plans to offer a fully managed platform solution for use as an integral part of customer application hosting environment. The offering will provide scalable database services including software license management, system database administration, server hardware and storage associated with the database. These services bundled together will provide required performance and functionality while delivering cost savings associated with the overall ease of management. OPM plans to offer various leading relational database platforms to ensure customers have adequate choice.

OPM PaaS-Dev/Test environments will offer two highly flexible development and test environments to rapidly develop applications. The dev/test environments will offer the tools that developers need to build their applications like development environments, web servers, application servers etc. OPM plans to offer various flavors of development environments for example LAMP and .Net.

All OPM PaaS services are built on OPM IaaS offerings and will include license management, system administration, application/web/database server patching in addition to the services offered in IaaS.

The primary benefits of OPM PaaS services:

- Simple to Deploy – OPM PaaS will make it easy for customers to go from project conception to deployment. It will enable the capabilities of a production-ready application/web/database server in hours/days without worrying about infrastructure provisioning or installing and maintaining database software.
- Managed – OPM PaaS will handle time-consuming management tasks, such as backups, patch management, and replication, so customers can pursue higher value application development or database refinements. The PaaS offerings will be monitored by the OPM staff and SLA reports will be provided to the customers.
- Scalable – OPM PaaS can be increased or decreased based on workload characteristics.
- Reliable – All OPM PaaS service offerings will inherit the same IaaS reliability features for availability, security and compliance. These services offer 99.99% availability and offer several high availability features.

All PaaS services are offered to the customers on an on-demand basis. So the customers only pay for the number of instances of PaaS service that are provisioned for them. The clarity and transparency offered in the PaaS model will allow OPM agencies to significantly reduce the amount they spend on software licenses. OPM will continue to consolidate the enterprise software licenses.

4.3. SaaS Services

“Software as a Service” (SaaS) is being adopted in multiple enterprise markets, such as CRM (for example, CRM on demand), human capital management (HCM; for example, performance management and recruitment), and workplace collaboration, procurement, e-mail and enterprise integration (for example, integration as a service). Each market that has adopted SaaS may use different terminology and may have variations in functionality. In a pure SaaS model, the provider delivers software based on a single set of common code and data definitions that are consumed in a one-to-many model by all contracted customers anytime, on a pay-for-use basis, or as a subscription based on use metrics. During the past few years, vendors have used multiple approaches to support the SaaS definition.

OPM Private SaaS offerings provide four key elements. They are service based, scalable, shared and priced by subscription/usage.

OPM will make the latest communication and collaboration tools available to its workers including Project Server, Primavera and Lync using a SaaS-based delivery approach. In addition, all these services will be charged on the subscription basis to the agency users.

OPM OCIO plans on leveraging several related efforts like Mobility Strategy to introduce new Private SaaS offerings that can be accessed through multiple devices including tablets and phones. OPM agencies that are working on business applications like Grants, Loans etc. shall look to offer business application capabilities as Private or Community SaaS to other agencies within OPM or to other agencies outside the department. Working with OCIO, the agencies can identify business application areas where they can be the technical leads and offer subscription based capabilities using OPM IaaS or PaaS offerings. OCIO envisions having a robust portfolio of Private SaaS based offerings available to OPM users on various devices; offered by OPM OCIO.

As more ISVs and SaaS providers develop and deploy SaaS applications, OPM end-users will be attracted towards low entry barriers for the Public or vendor provided SaaS solutions. Given that the security, data confidentiality and integrity requirements around government data remain at the forefront of importance; it is extremely important that adoption of Public SaaS solutions be guided by OMB, GSA and OPM OCIO efforts and frameworks like the Cloud Applicability framework described below.

The OMB’s Federal Risk and Authorization Management Program or FedRAMP has been established to provide a standard approach to Assessing and Authorizing (A&A) Cloud computing services and products. FedRAMP will allow joint authorizations and continuous security monitoring services for Government and Commercial Cloud computing systems intended for multi-agency use. Joint authorization of Cloud providers results in a common security risk model that can be leveraged across the Federal Government. The use of this common security risk model provides a consistent baseline for Cloud based technologies. This common baseline will ensure that the benefits of Cloud-based technologies are effectively integrated across the various Cloud computing solutions currently proposed within the government. The risk model will also enable the government to "approve once, and use often" by ensuring multiple agencies gain the benefit and insight of the FedRAMP's Authorization and access to service provider’s authorization packages. OPM agencies must work with the vendors that are participating with the FedRAMP initiative and/or have received FISMA certification for the specific offering that the agency plans to use.

5. Agency Cloud Applicability Framework

Cloud based applications and/or services are rapidly being introduced in the market place by vendors. The constantly changing vendor landscape as well the differing capabilities offered by them makes it challenging for consumers of Cloud services to identify when and what services are good fit for what type of Cloud offering.

OCIO Cloud decisions will be based on the individual workload characteristics. To help OPM make informed Cloud computing decisions, OPM OCIO has adopted a Cloud Applicability Framework based on the OMB's Decision Framework for Cloud Migration. It is important that OPM decisions are based on business value drivers and risk profile.

The OPM Cloud Applicability Framework takes three primary factors to help OPM agencies plan their Cloud migration. These primary factors are:

1. ***Value -*** measures Cloud effects on customer's current efficiency, agility, and innovation
2. ***Readiness -*** captures the ability for the IT service to move to the Cloud in the near-term; the primary differentiators are security, elasticity needs, service level requirements, and data confidentiality
3. ***Market Availability*** - captures the availability of federally compliant Cloud based services in the market place

OCIO has identified the following workloads as good candidates for Cloud computing:

- **Public Data** – OPM today manages several external websites, most of them have some dynamic data, reports for public consumption and some static content. Right now OPM web sites are not used to disseminate live speeches of the OPM leadership. Cloud offerings will allow us to offer these types of content rich offerings to the Public through public Cloud content delivery network (CDN) services. Cloud providers have successful track records for offering rich content that is often in high demand for a very short period of time.
- **External Collaboration** – Leveraging a public, hybrid Cloud for external collaboration provides significant benefits as it relates to time to market of a solution that is "always on" allowing connectivity from anywhere. This Cloud solution leverages existing investments, and would extend our collaboration capabilities beyond the firewall, require minimal user training, and would be accessible from personal devices.
- **Research Data Sets** – OPM Research areas purchase several public data sets for various types of analysis. These research sets are often very large and are used for a small period of time while the researchers conduct their analysis. These types of workloads that require large amount of storage and compute capability for a small period of time are excellent candidates for public Clouds. Hybrid Clouds can be used for research data sets that have moderate security requirements because at this time the security controls in the public Cloud are not strong enough to support moderate security Research datasets. Further, OCIO does not recommend using Cloud solutions for datasets with high security requirements.

- **Application Development, Test** – Application development teams across the System need several environments during the development/test phase of their projects. The capital investment required and the lead time for setting up each environment requires application teams to use creative ways of managing these environments including moving data sets between environments at night. Easier access to the development and test environments as needed, will significantly improve the productivity of the development teams.

  Given the sensitivity of the development and test data sets (PII), public Cloud offerings are not yet recommended for Application Test and QA workloads. Hybrid Cloud may be a possibility for Development and Test environments in the future, but at this time OCIO recommends using the OPM Private Cloud for these capabilities.

- **Production Application** – While OCIO recommends using virtualized environments for production workloads, at this time we do not recommend using Cloud computing for these workloads. While production environments have elasticity needs, their computing needs are more predictable and will not benefit from the using pay-as-you-go approach. Also, the SLA requirements for production workloads make them a less attractive candidate for Cloud computing.

6. OPM Cloud Computing Roadmap

This section provides a high-level implementation plan based on the analysis of information obtained and recorded in the "OPM Cloud Computing Strategy Assessment Report." Recommendations based on this analysis are included as a guide for embracing cloud computing throughout OPM. Table 3-1 provides a summary of the plan.

Table 6-1 Implementation Plan Summary

Action Item	Start Time after Project Initiation	Action
1	Ongoing	Consolidate and optimize current environment
2	Immediate	Publish and publicize OPM Cloud Strategy
3	Immediate	Establish a CIO-level technology review committee
4	Immediate	Consolidate development and operations oversight at CIO-level
5	Immediate	Evaluate current skills compared to cloud operations
6	Immediate	Document current services in use by OPM
7	6 months	Develop a service catalog
8	6 months	Review available cloud contract vehicles
9	6 months	Map business needs to available cloud services

Action Item	Start Time after Project Initiation	Action
10	6 months	Review budget process
11	6 months	Identify and vet cloud providers
12	7 months	Identify potential cloud candidates
13	7 months	Build cloud cost and ROI models for potential cloud candidates
14	7 months	Conduct impact analysis
15	9 months	Communicate cloud services options, roadmap, potential changes to decision makers
16	9 months	Pilot: Use cloud services
17	Immediate	Document current services offered to other Government agencies
18	6 months	Establish contract vehicle(s) for OPM to offer cloud services
19	9 months	Pilot: Deliver cloud services

7. Next Steps

OPM OCIO will continue to refine the current OPM Cloud Strategy. In order to achieve this, the team will:

- Initiate a deep dive analysis of the current IT infrastructure across all of OPM's Data Centers
- Evaluate the areas within the various OPM data centers that can be quickly migrated to the OPM Private Cloud
- Expand and refine the current Cloud roadmap for OPM and leverage new technologies to determine the optimum path to the Cloud