



Cloud/SaaS Policy Review

Reference Guide

SPRING 2014

The Federal Government has established a number of policies and procedures regarding the acquisition and deployment of SaaS/Cloud solutions. This paper serves as a Reference Guide for SaaS/Cloud research and analysis under government guidelines.



Table of Contents

INTRODUCTION.....	3
SECTION 1 SAAS/CLOUD POLICY OVERVIEW	4
1.1 History of Cloud Policy	4
1.2. Why Cloud?	6
1.2.1 Cost Reduction.....	7
1.2.2 Speed and Flexibility.....	7
1.2.3 Greater Mobility	8
1.2.4 Easier Collaboration.....	8
1.2.5 Heightened Security	9
1.3. Areas of Concern	9
1.3.1 Cost Reduction.....	10
1.3.2 Flexibility.....	11
1.3.3 Greater Mobility	12
1.3.4 Easier Collaboration.....	12
1.3.5 Heightened Security	12
1.4. The Four Cloud Types.....	13
1.4.1 Public Clouds.....	15
1.4.2 Private Clouds.....	15
1.4.3 Hybrid Clouds.....	15
1.4.4 Community Clouds	15
SECTION 2 FEDERAL CIO POLICY	16
2.1. Historical Perspective	16
2.2. OMB 25-Point Plan Removes Government IT Barriers	17



Reference Guide: Cloud / SaaS Policy Review

2.2.1 Strengthen Program Management	18
2.2.2 Align the Acquisition Process with the Technology Cycle	19
2.2.3 Align the Budget Process with the Technology Cycle	19
2.2.4 Streamline Governance and Improve Accountability	20
2.2.5 Increase Engagement with Industry	20
2.2.6 Funding and Security	21
2.3. Additional Articles on Federal CIO Cloud First Policy.....	21
SECTION 3 DOD CIO POLICY	25
3.1. DoD Cloud Computing Strategy	25
SECTION 4 GSA OVERSIGHT	28
4.1. GSA's Mission for Cloud Computing	28
4.2. FedRAMP	29
4.2.1 Guide to Understanding FedRAMP	29
4.2.2 Mandatory Program for Using Cloud Service Providers.....	30
4.3. GSA Recommendations for Effective Cloud Agreements	30
4.4. GSA's Cloud Migration SOO Templates.....	31
4.5. Additional Resources.....	32

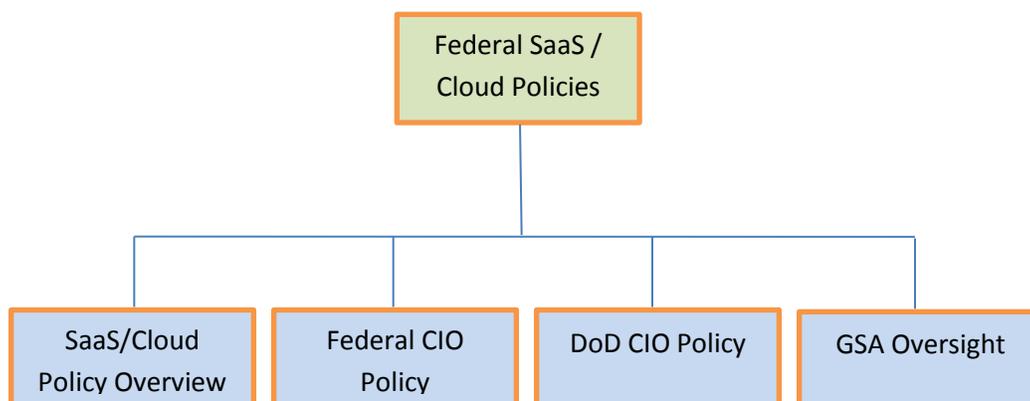


Reference Guide: Cloud / SaaS Policy Review

INTRODUCTION

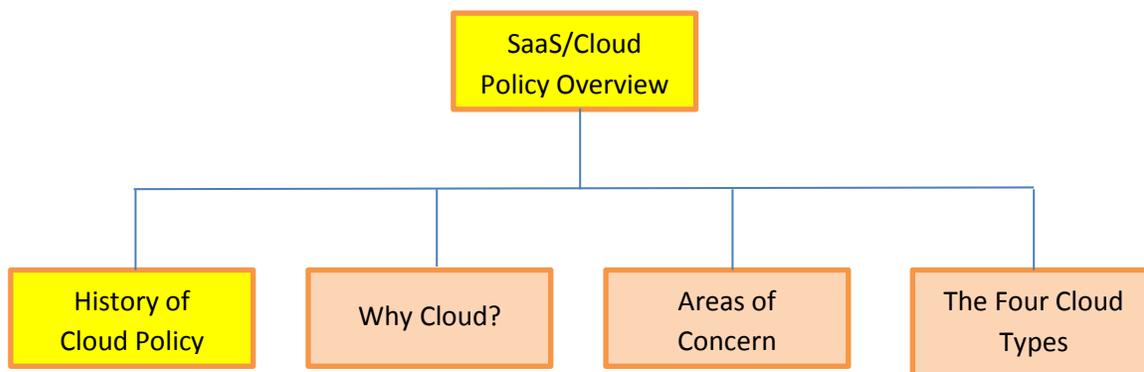
The Federal Government has established a number of policies and procedures regarding the acquisition and deployment of SaaS/Cloud solutions. This Advisory Note serves as a Reference Guide for SaaS/Cloud decision making. It covers four aspects of SaaS/Cloud policies:

1. History of Cloud Policy
2. Why the government views SaaS/Cloud as important technologies
3. Major areas of concern when acquiring and deploying these technologies
4. Major types of Cloud deployments.





SECTION 1 SAAS/CLOUD POLICY OVERVIEW



This section is a high level overview of SaaS/Cloud Policy history. Detailed information can be found in sections 2 throughout the remainder of this paper.

Policy statements from the Federal CIO, DoD CIO, GSA and OMB provide guidance regarding acquisition and deployment of new technologies, including SaaS/Cloud. Many government agencies and officials opined on the pros and cons of SaaS/Cloud for some time before formal policy statements were made and actions taken.

1.1 History of Cloud Policy

One of the pre-cursors to a formal SaaS/Cloud policy was the movement to consolidate government IT infrastructure. SaaS/Cloud computing strategy and policy are closely related to several important factors:

The government's desire to cut costs where possible, including the annual \$80 billion IT budget.

The government's desire to borrow from commercial best practices where it makes sense, including the deployment of new technologies such as virtualization, Cloud and SaaS.

The government's desire to combine those two factors to consolidate and reduce federal IT infrastructure.



Reference Guide: Cloud / SaaS Policy Review

As a step in realizing those objectives, the Federal CIO made an announcement in February 2010 regarding data center consolidation:

In February 2010, the Federal CIO announced the Federal Data Center Consolidation Initiative. In it, he designated two Federal agency CIOs -- Richard Spires (DHS) and Michael Duffy (Treasury) – to lead the effort inside the Federal CIO Council. It also highlighted the following goals:

- *Reduce the cost of data center hardware, software and operations*
- *Increase the overall IT security posture of the government*
- *Shift IT investments to more efficient computing platforms and technologies*
- *Promote the use of Green IT by reducing the overall energy and real estate footprint of government data centers*

- From the statement of Dr. David McClure, Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration, before the House Committee on Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement, July 1, 2010

<http://www.gsa.gov/portal/content/159101>

The first official pronouncements specifically discussing cloud computing came in November 2010 when the chief performance officer of OMB, Jeffrey Zients, announced that OMB, as a critical part of its 25 point plan for IT modernization, will require federal agencies to default to cloud solutions under certain circumstances.

The November 2010 OMB announcement was quickly followed on December 9, 2010 by the now famous “Cloud First” policy enunciated by Vivek Kunda, Federal CIO at the time.

In October 2011, Kunda’s successor, Steven van Roekel, took the cloud first policy to another level, referring to it as “Future First.” See <http://www.parc.com/event/1613/evening-with-steven-vanroekel.html>

In July 2012, DoD CIO Teri Takai released a comprehensive DoD Cloud strategy document after having released her DoD 10 point plan for modernizing the IT infrastructure in January 2012. See <http://www.defense.gov/news/DoDCloudComputingStrategy.pdf>



Reference Guide: Cloud / SaaS Policy Review

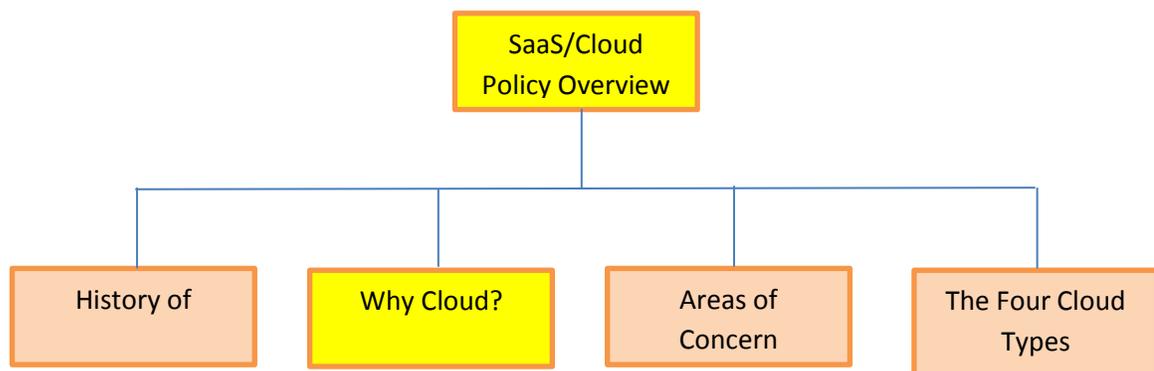
FedRAMP, a government-wide program governing security concerns related to government use of cloud computing is overseen by GSA. It was initially introduced in an OMB Policy Memo dated December 8, 2011. See the following document on line:

http://www.gsa.gov/graphics/staffoffices/FedRAMP_3PAO_Industry_Day_FedRAMP_Overview.pdf

On the GSA website, the following short description is provided:

“FedRAMP is the result of close collaboration with cyber-security and cloud experts from GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council and its working groups, as well as private industry.” (<http://www.gsa.gov/portal/category/102375>)

1.2. Why Cloud?



Aside from the OMB and other directives to use Cloud First, there are five business reasons often cited for the DoD and others to take advantage of cloud computing:

1. Cost reduction
2. Speed and flexibility
3. Greater mobility
4. Easier collaboration
5. Heightened security

This section will examine each reason and list some of the potential benefits to consider when evaluating cloud proposals versus more traditional licensing models.



Reference Guide: Cloud / SaaS Policy Review

1.2.1 Cost Reduction

SaaS or Cloud licenses generally provide all software and services needed to operate a business application, including:

- a. Application & Related Software Licenses
- b. Maintenance (fixes, patches, upgrades) & Support
- c. Infrastructure & Facilities

The potential for cost savings is obvious. Hardware and other infrastructure and facilities costs can be shared across multiple entities in a Cloud/SaaS arrangement. Virtualization and other technologies can facilitate the optimization of resources not only within an enterprise but also across many of them. The Government licensee can participate in these efficiencies when buying SaaS licenses.

While license fees themselves are generally not “shareable” across enterprises, there are still potential savings stemming from certain license features. Licensees can negotiate for fees based only on numbers of actual users or other use metrics instead of locking themselves into a set (and often poorly estimated) number of users in a perpetual license.

The nature of a subscription-based license assumes an annual cost based on some hypothetical amortization of the license and services. Instead of paying a large fee at contract time with annual maintenance and support payments, the subscription approach results in a lower and more predictable annual cost. This can be especially beneficial when licensing software for relatively short periods of time.

In summary, when comparing total costs for subscribing to a Cloud /SaaS bundled offering to a traditional model, the subscription price over the expected life of the subscription license is likely to be less than the cost to purchase/license the components in the traditional model. The reason is fairly straightforward – the cloud provider can pass along the savings enjoyed from leveraging the various components across multiple customers.

1.2.2 Speed and Flexibility

Using a Cloud or SaaS offering can provide more flexibility than a traditional model in several ways. Probably the most important benefit in this category is the reduced time and cost of deployment compared to perpetual licenses for complex software applications such as ERP apps. Closely associated



Reference Guide: Cloud / SaaS Policy Review

with those reduced costs are the significantly reduced time and costs for the procurement of Cloud/SaaS versus perpetual licenses.

Other aspects in this category include the ability to add or subtract subscribers on a monthly or quarterly basis, depending on the terms negotiated in the license agreement. This can save time and money in audits and non-compliance.

Another related feature is the timely provisioning of new users. Cloud vendors typically have a streamlined process to onboard new users or delete those no longer permitted to have access to the system.

The broad use of virtualization in Cloud Service Provider (CSP) environments also contributes to the speed and flexibility of using Cloud/SaaS. Since most CSPs service many customers from a single environment, virtualization allows for much more efficient use of hardware and software resources, essentially sharing them across customers.

1.2.3 Greater Mobility

The primary mobility benefit is found in the “out-of-the-box” readiness of most Cloud/SaaS environments to handle virtually all mobile devices on the market. This makes connectivity from any location simple and cheap. It prevents each customer from having to spend money on multiple technologies to enable mobility and especially reduces the requirements for hiring personnel knowledgeable in the various technologies available today. The Cloud/SaaS provider can amortize these costs across all customers as they do with others.

1.2.4 Easier Collaboration

Cloud/SaaS offerings enable collaboration in two key ways:

- a. CSPs deliver previously developed and tested APIs for easy connection to multiple applications
- b. Many CSPs not only deliver the APIs but also deliver integrated solutions out of the box, thereby avoiding the need for the licensee to integrate the applications.



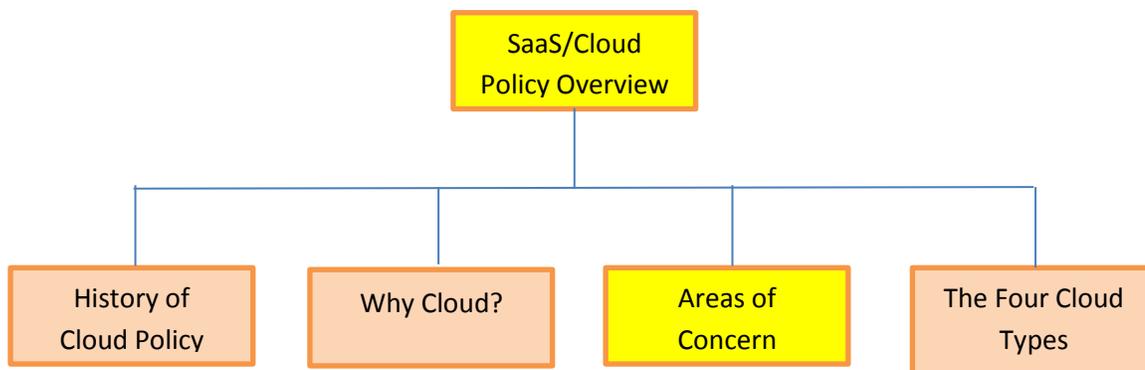
1.2.5 Heightened Security

The need for tight security around systems, data, facilities and people is well understood today. It can be argued the government requires an even higher standard for security than most commercial firms. To meet these security needs, CSPs take a number of steps to provide licensees with adequate assurances:

- a. Most cloud servers are hosted in physically secure data centers with strict access control for their own staff and no access for unauthorized personnel.
- b. CSPs can hire top security talent and amortize those costs across multiple customers.
- c. CSPs can also deploy the most advanced cyber-security devices and applications.
- d. CSPs often have cutting-edge, secure, and traceable data access trails.

The government has created a robust set of recommended contract clauses focused on its security needs with specific duties imposed on CSPs. (See the Best Value Toolkit’s “Agreements” tab.)

1.3. Areas of Concern



As stated in “Why Cloud?” there are five business reasons often cited for DoD and others to take advantage of cloud computing:

1. Cost reduction



Reference Guide: Cloud / SaaS Policy Review

2. Speed and flexibility
3. Greater mobility
4. Easier collaboration
5. Heightened security

While each of these business reasons can provide potentially large benefits as discussed in “Why Cloud?” it is important to analyze each one to understand whether and how the potential benefits might be realized. This section will examine each benefit with some questions designed to challenge their expected value.

1.3.1 Cost Reduction

SaaS or Cloud licenses generally provide all software and services needed to operate a business application, including:

- a. Application & Related Software Licenses
- b. Maintenance (fixes, patches, upgrades) & Support
- c. Infrastructure & Facilities

How can you tell whether corresponding internal costs will be avoided or go away? What happens to your cost model if they don't go away or costs of buying/licensing them are not avoided?

- a. Will you end up paying twice for certain items (e.g. servers) if they do not leave your internal environment as a direct result of a SaaS license?
- b. How do you know a SaaS cost is lower than an internal cost for an item?
- c. Since you may license a variety of applications from a variety of SaaS vendors, do the economies of scale from each vendor outweigh the aggregate internal economies if you hosted all those apps on premises?

Another important factor to consider in evaluating cost is the vendor's time horizon for amortizing its investments in the components it uses to provide services to customers via its subscription price. If your time horizon is longer than the vendor's (as is often the case in the government), you will likely pay more for the offering than the vendor planned to recoup in cost and profit. A simple example will help illustrate the principle:



Reference Guide: Cloud / SaaS Policy Review

Assume the vendor's cost for software, hardware, facilities, etc. is \$2 million. Assume the vendor determines a five-year amortization is appropriate for pricing – and assume the vendor plans to make a 25% profit. The total cost plus profit is \$2.5 million, so the vendor would likely set its annual price at \$0.5 million, planning to recoup all costs plus profit over the expected five-year time horizon it has estimated as the standard or average time horizon in the marketplace.

Now let's assume you can buy/license the same components at a price 25% higher than the vendor can (due to the vendor's volume buying) – and that your time horizon for using the software is actually seven years.

In this example your total cost is identical to the vendor's. Your cost to buy directly is \$2 million plus the 25% premium due to lack of buying power (the government can probably overcome this) for a total of \$2.5 million – the exact same price as the total planned subscription from the vendor based on their five year horizon. If the vendor price is based on that approach, it will be \$0.5 million (as above). Your annual cost for the same components will be the \$2.5 million divided by seven years, or about \$0.355 million per year. Although the total costs are the same, your annual cost is \$0.145 million less than the subscription price. Another way to look at this set of facts is that you would have the same capabilities two years longer than the vendor's offer for the same amount of money.

1.3.2 Flexibility

Although the common wisdom says Cloud/SaaS is more flexible than traditional perpetual licenses (as described in the section, 'Why Cloud?'), there are some important questions to ask and answer before assuming Cloud/SaaS provides superior flexibility.

While switching costs from one SaaS vendor to another could be less than switching from one perpetual vendor to another for the same application, would it be as easy to switch ERP SaaS vendors as it might be for email providers?

What about customization? Most Cloud/SaaS arrangements severely limit the licensee's ability to request and obtain customizations, whether receiving services from true multi-tenant SaaS environments or from those not truly offering multi-tenant capabilities. Traditional perpetual licenses afford the opportunity to make as many customizations as desired – and they can be as complex as required.



Reference Guide: Cloud / SaaS Policy Review

What about control over the timing of upgrades? Most Cloud/SaaS arrangements place the timing and types of upgrades solely at the discretion of the licensor. The application, interface and customization testing, training and other readiness tasks associated with upgrades should not be overlooked. While the licensee might be okay with upgrading every two years, for example, the licensor probably will want to upgrade with every new release which could mean every six to nine months.

Is virtualization limited to the cloud? Although Cloud/SaaS providers tout their virtualization capabilities as a source of cost savings and flexibility, licensees should understand the incremental increase in value, if any, over and above that which they can achieve in their own environments.

How do you put a price on flexibility gained or lost? The key here is to ask the right questions and to put a number on the pros and cons of flexibility gained or lost with Cloud/SaaS arrangements.

1.3.3 Greater Mobility

As with some elements of flexibility, Licensees should ask whether the mobility benefits offered by Cloud/SaaS providers are necessary for Licensees' needs – then they should ask whether those benefits can be obtained as easily and cheaply in the Licensees' own environments as they are in the Cloud/SaaS environments.

1.3.4 Easier Collaboration

The same can be said for alleged collaboration benefits. There are probably no capabilities offered by Cloud/SaaS providers that can't be achieved in licensee-managed environments. The real question is whether they can be achieved as efficiently and cost effectively with one versus the other.

1.3.5 Heightened Security

Perhaps more important than the matter of alleged cost reduction is the notion that Cloud/SaaS arrangements offer security capabilities superior to those achievable by Licensees in their own environments. A detailed treatment of security matters can be found at the following websites:



Reference Guide: Cloud / SaaS Policy Review

<http://www.gsa.gov/portal/category/102375>

http://www.microsoft.com/industry/government/guides/cloud_computing/3-security.aspx

<http://www.csoonline.com/article/717307/5-more-key-cloud-security-issues>

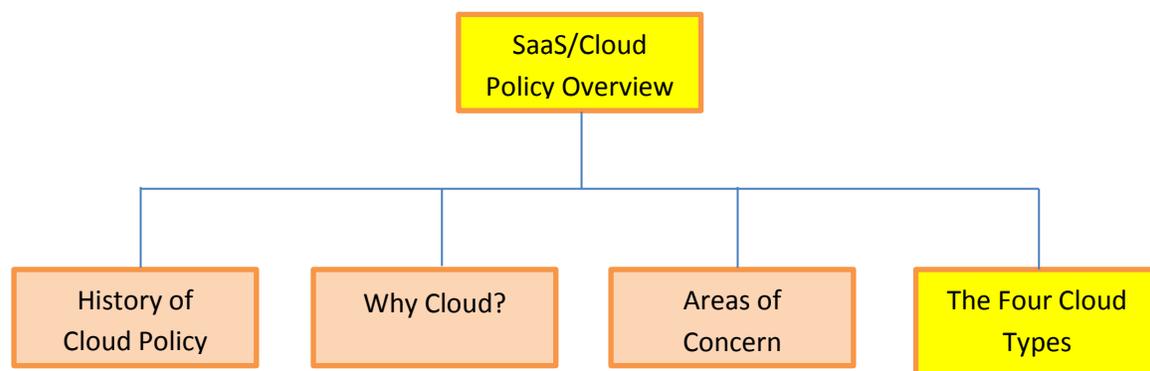
<http://www.eweek.com/c/a/Security/RSA-Conference-Security-Issues-From-the-Cloud-to-Advanced-Persistent-Threats-771644/>

<https://www.securityweek.com/addressing-cloud-security-concerns-key-issues-and-recommendations>

<http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues>

A key point in this section is to ask the right questions about the security measures available from the CSP – and the associated costs for those measures. Additionally, make sure the appropriate contract obligations are included in Cloud Service or SaaS Agreements to require the necessary safeguards over systems and data, along with SLAs and mechanisms for measuring compliance. The Federal Cloud Compliance Committee’s recommended clauses are a good reference point.

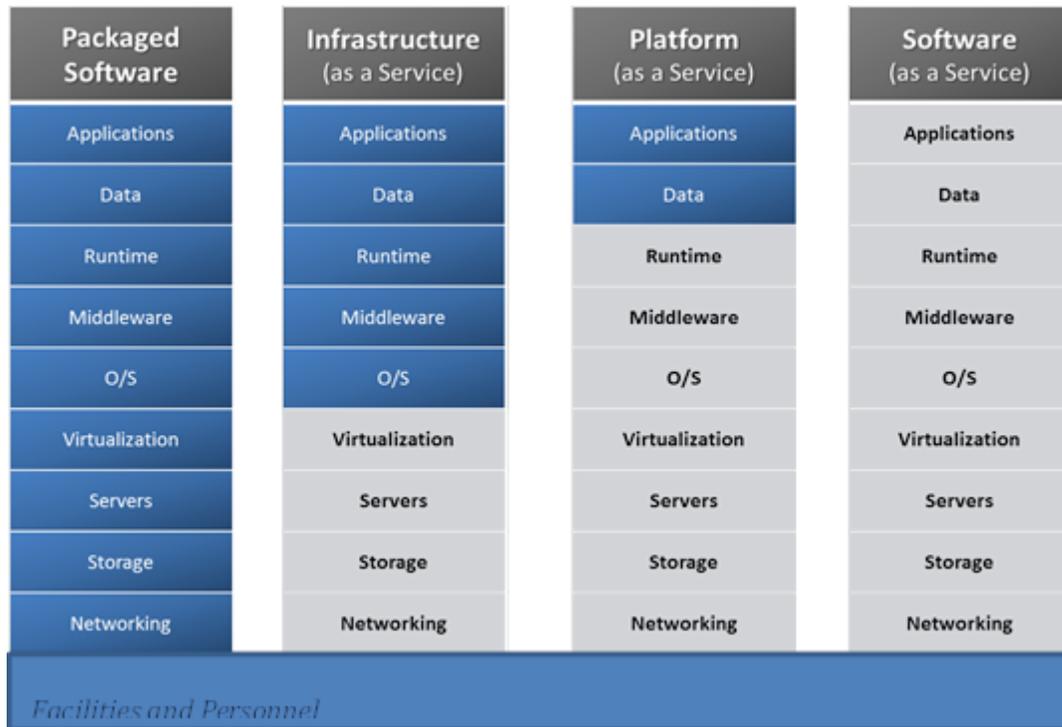
1.4. The Four Cloud Types





Reference Guide: Cloud / SaaS Policy Review

A typical cloud environment includes several layers of infrastructure and software built on a foundation of facilities and people with appropriate expertise.



In the diagram below, the four major types of cloud are depicted along with the key attributes of each.

Public	Community	Private	Hybrid
Off premise at provider	On or off premise	On or off premise	On or off premise
General public	Multiple, related organizations	Limited to a single organization	Determined by each cloud
Users' concerns and purposes vary	Users share the same concerns	Used by various business units	Users' concerns and purposes vary



Reference Guide: Cloud / SaaS Policy Review

1.4.1 Public Clouds

Public Clouds are provided by commercial enterprises who offer cloud computing services to customers generally. In a public cloud, the IT resources can be optimized to the fullest extent possible since by definition, there are no resources dedicated to a single customer. Also by definition, the services are provided off premises from the customer.

Entities using public clouds should pay particular attention to the security concerns discussed in the previous section on “Areas of Concern.”

1.4.2 Private Clouds

Private Clouds can be created on premises by an organization seeking to enjoy the benefits of cloud computing (e.g., the government can create its own private cloud) or the cloud can be provided on premises or off premises by a cloud service provider (CSP). The key difference between a public and private cloud is apparent from their names – a public cloud can be shared by several entities while a private cloud’s resources are dedicated to a single customer.

1.4.3 Hybrid Clouds

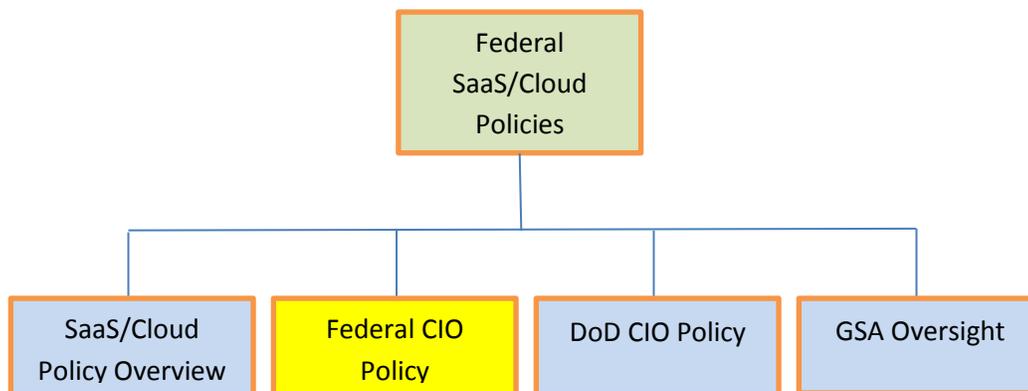
Hybrid Clouds have elements of both public and private clouds. Some pieces of the infrastructure are shared and some are dedicated to a single entity. Probably the most popular combination is to have all infrastructure pieces available to several entities except for the database software and the data storage server. This combination is thought to provide higher security for data while taking advantage of the optimization and associated savings for the rest of the infrastructure.

1.4.4 Community Clouds

Community Clouds can be thought of as a limited public cloud or an extended private cloud. It is a set of cloud resources dedicated to a group of organizations who share common business interests or common concerns. Only members of the community can use the resources, so there is more exclusivity than a public cloud but less than a private cloud dedicated to a single entity.



SECTION 2 FEDERAL CIO POLICY



This section captures the content of key articles documenting Federal CIO Policy, primarily excerpts from an article titled “OMB announces 25-point implementation plan for restructuring federal IT,” which first appeared on the *Fierce Government IT* website on December 9, 2010. This article is available at <http://www.fierceregovernmentit.com/story/omb-announces-25-point-implementation-plan-restructuring-federal-it/2010-12-09>.

2.1. Historical Perspective

As Cloud Computing grew in popularity and importance, the Federal Government began to explore the potential benefits it could provide to government users as well as the potential for reduced spending. The initial impetus for moving to the cloud was as much a cost-saving strategy as it was a technology strategy.

By way of background, it is interesting to note that the Defense Information Systems Agency (DISA) is the primary provider of technology infrastructure to the government. DISA is the successor organization to the Defense Communications Agency which was established in 1960. The name was changed to DISA in 1991. (See <http://disa.mil/About/Our-History> for a history of DISA.)

As computing requirements grew, DISA’s resources also expanded rapidly. It became apparent that the costs in personnel, equipment, technologies, real estate and associated inefficiencies



Reference Guide: Cloud / SaaS Policy Review

dictated that alternatives needed to be found. The government began a data center consolidation program before announcing a “Cloud First” policy in 2009/2010.

The cited *Fierce Government IT* article, written by Molly Bernhart Walker, starts with a statement attributed to Jeffery Zients, the OMB’s Deputy Director of Management and Federal Chief Performance Officer:

Zients said OMB's 25-point implementation plan will help remove the barriers that consistently get in the way of successful project management and execution. The 25 points are [based on five broad changes to agency IT](#), outlined by OMB on Nov. 22[2010]: Adopting light technologies and shared services; aligning the budget and acquisition process with the technology cycle; strengthening program management; streamlining governance and increasing accountability; and, increasing engagement with the IT community.

Mr. Zients’ points clearly favor cloud services as a means of relieving government of the tremendous burden of providing infrastructure and application support to the hundreds of thousands of government IT consumers.

2.2. OMB 25-Point Plan Removes Government IT Barriers

The entire 25-point plan as documented in the *Fierce Government IT* article is included here to provide an accurate historical perspective on the initialization of the “Cloud First” policy as announced at the Federal CIO level in 2010.

The entire shared services strategy within federal government is being revisited said Vivek Kundra, federal chief information officer. The goal, he said, is to have something like online restaurant reservation website [Open Table](#), but for data centers. If one agency needs more space and another has it, the first agency can use that space already available within government rather than purchasing that capability, Kundra said. Below are the OMB action items that apply to technology adoption.

	Action Item	Owners	Within 6 mos	6-12 mos	12-18 mos
1	Complete detailed implementation plans to consolidate 800 data centers by 2015	OMB, Agencies	X		
2	Create a government-wide marketplace for data center availability	OMB, GSA			X
3	Shift to a "Cloud First" policy	OMB, Agencies	X		



Reference Guide: Cloud / SaaS Policy Review

4	Stand-up contract vehicles for secure IaaS solutions	GSA	X		
5	Stand-up contract vehicles for "commodity" services	GSA		X	
6	Develop a strategy for shared services	Federal CIO		X	

2.2.1 Strengthen Program Management

There is currently no career track within government for project management, said Kundra. These workers have no community for sharing best practices and lack appropriate training and tools, he said, adding that his office will work with Office of Personnel Management to create a distinct career path with direct hiring authorities. A pilot program will start immediately, Kundra said.

He also advocated a technology fellows program where people could join an agency for six-month stints to share ideas. This would be an option for young workers--training the next generation of civil servants--and for industry professionals to join government to share ideas and work on implementing new technology. Below are the action items that apply to program management.

	Action Item	Owners	Within 6 mos	6-12 mos	12-18 mos
7	Design a formal IT program management career path	OPM, OMB	X		
8	Scale IT program management career path	OPM, Agencies			X
9	Require Integrated Program Teams	OMB	X		
10	Launch a best practices collaboration platform	Federal CIO Council	X		
11	Launch technology fellows program	Federal CIO		X	
12	Enable IT program manager mobility across government and industry	OMB, CIO Council, OPM			X



Reference Guide: Cloud / SaaS Policy Review

2.2.2 Align the Acquisition Process with the Technology Cycle

The White House plans to change several aspects of the acquisition process. First, it hopes to develop a cadre of specialized acquisition professionals. It also aims to stand up templates that support modular development. Kundra also said OMB is “going to enact a set of policies that will attract those innovative companies that want to do business with the federal government.” Below are the action items that apply to improved acquisition.

	Action Item	Owners	Within 6 mos	6-12 mos	12-18 mos
13	Design and develop cadre of specialized IT acquisition professionals	OMB, Agencies	X		
14	Identify IT acquisition best practices and adopt government-wide	OFPP	X		
15	Issue contracting guidance and templates to support modular development	OFPP		X	
16	Reduce barriers to entry for small innovative technology companies	SBA, GSA, OFPP			X

2.2.3 Align the Budget Process with the Technology Cycle

The budget cycle often requires agencies to predict in some detail what technology they will need two years down the road. Kundra said OMB will work with Congress over the next few months to create budget models that support agile software development. These reforms will ensure agencies don't throw good money after bad just because they're afraid of losing funding, he said. Below are the action items that apply to budget process reform.

	Action Item	Owners	Within 6 mos	6-12 mos	12-18 mos
17	Work with Congress to create IT budget models that align with modular development	OMB, Agencies	X		
18	Develop supporting materials and guidance for flexible IT budget models	OMB, CFO & CIO Councils		X	
19	Work with Congress to scale flexible IT budget models more broadly	OMB, Agencies			X
20	Work with Congress to consolidate Commodity IT spending under Agency CIO	OMB, Agencies	X		



Reference Guide: Cloud / SaaS Policy Review

2.2.4 Streamline Governance and Improve Accountability

Kundra said OMB has had to go through seven or eight layers of governance, during TechStat meetings to find the person actually responsible for an IT system. This has created what he calls “a culture of faceless accountability,” in that if everyone's accountable, no one is accountable. Kundra also said OMB will have to fundamentally rethink the agency CIO's job, so CIOs can focus less on policy and more on portfolio management. Below are the action items that apply to governance and accountability.

	Action Item	Owners	Within 6 mos	6-12 mos	12-18 mos
21	Reform and strengthen Investment Review Boards	OMB, Agencies	X		
22	Redefine role of Agency CIOs and Federal CIO Council	Federal CIO, Agency CIOs	X		
23	Rollout "TechStat" model at bureau-level	Agency CIOs			X

2.2.5 Increase Engagement with Industry

"We need to be crystal clear on what our requirements are and we need to be crystal clear on what's not working," said Kundra in reference to public-private partnerships. "We want to make sure that the platform allows us to get innovative ideas early." OMB has tapped Daniel Gordon, administrator for federal procurement policy within OMB, to lead a 'myth-busting' campaign.

"We need to take better advantage of flexibilities we already have," said Gordon, during the press briefing. He added that it is not necessary to make new statutes or changes to Federal Acquisition Regulation because "procurement reform in the 1990s gave us the tools [we need] to do this...now we need to really make this happen in execution."

	Action Item	Owners	Within 6 mos	6-12 mos	12-18 mos
24	Launch "myth-busters" education campaign	OFPP	X		
25	Launch an interactive platform for pre-RFP agency-industry collaboration	GSA	X		



Reference Guide: Cloud / SaaS Policy Review

2.2.6 Funding and Security

If these 25 points are implemented correctly, said OMB officials, major gains will be made in federal IT. However, one point was noticeably absent from the discussion: Additional funding for projects. As for the federal acquisition corps, Gordon said he is working with agencies to find ways to get the training done within the budget agencies have today. OMB is also working with congress to add money in this area, but it is unlikely budgets will loosen anytime soon, he added.

Other IT items excluded from the implementation plan include any formal mention of telecom or cybersecurity. OMB considers telecom as “commodity IT,” said Kundra, and cybersecurity is not a single item to touch on, but an encompassing concern for all parts of agency IT restructuring.

Teri Takai, CIO at the Defense Department made a request of Kundra toward the end of the meeting, “that we really look at the cybersecurity aspects as important as our innovation and efficiency drives.” She added that security could become an unintentional trade off with the rapid implementation being demanded of agencies.

Kundra assured Tekai that security is “vital” to the plan and “baked in.”

2.3. Additional Articles on Federal CIO Cloud First Policy

A series of articles from 2010 through 2013 are presented below to highlight the significance of the Federal CIO Cloud First policy.

1. “Cloud-First Policy—What Does It Really Mean”
2. “Federal government moves forward with ‘cloud first plan for new technology”
3. “U.S. Department of Commerce Office of the Chief Information Officer Cloud Computing Policy
4. “US government adopts ‘cloud first’ policy”
5. “OMB announces ‘cloud first’ policy for agencies”
6. “U.S. CIO VanRoekel Outlines What’s Next for Fed Tech”
7. “An Interview with Federal CIO Steven VanRoekel on the Future of Computing”

Notice the thrust of the Cloud First policy announcement and reasons for going to the cloud (expected increases in efficiency and reductions in cost).



Reference Guide: Cloud / SaaS Policy Review

1. “Cloud First Policy -- What Does It Really Mean?”

Dan Lohrmann, *Government Technology* only article, December 19, 2010

<http://www.govtech.com/blogs/lohmann-on-cybersecurity/Cloud-First-Policy--121910.html>

The federal government has issued a “cloud first” policy as a part of the Office of Management and Budget's [25-point plan to reform federal information technology management](#). The policy was described by federal CIO Vivek Kundra during a [December 9, 2010 presentation](#). This cloud first policy was presented as an important aspect of government reform efforts in order to achieve operational efficiencies by adopting “light” technology and shared services.

2. “Federal government moves forward with ‘cloud first’ plan for new technology”

Marjorie Censer, *The Washington Post* article, December 5, 2010

<http://www.washingtonpost.com/wp-dyn/content/article/2010/12/05/AR2010120503320.html>

The push for Web-based computing is part of a broader government effort to consolidate its 2,100 data centers by at least 40 percent by 2015.

3. “U.S. Department of Commerce Office of the Chief Information Officer Cloud Computing Policy”

U.S. Department of Commerce Website

http://ocio.os.doc.gov/ITPolicyandPrograms/Policy_Standards/PROD01_009505

Beginning with the FY 2012 budget, the Office of Management and Budget requires that Federal agencies consider Cloud Computing as an alternative for new IT investments. For the FY 2013 budget, the requirement to consider Cloud Computing covers mixed lifecycle projects (those that include development, modernization, and enhancement as well as steady state operations), and in FY 2014, the requirement covers all projects.

4. “US government adopts ‘cloud-first’ policy”

Joe McKendrick, *SmartPlanet* “Business Brains” online blog, November 30, 2010

<http://www.smartplanet.com/blog/business-brains/us-government-adopts-cloud-first-policy/>

The Washington Post’s Marjorie Censer reports that US federal agencies are now required to adopt a “cloud-first” policy when considering new information technology purchases. The policy is the result of an overhaul of the government’s IT procurement process:



Reference Guide: Cloud / SaaS Policy Review

“Jeffrey Zients, the federal government’s first chief performance officer, announced... that the Office of Management and Budget will now require federal agencies to default to cloud-based solutions ‘whenever a secure, reliable, cost-effective cloud option exists.’”

5. “OMB announces ‘cloud first’ policy for agencies”

Federal News Radio, 1500 AM, November 23, 2010

<http://www.federalnewsradio.com/?sid=2129860>

Big news this week on the cloud computing front. Agencies are being [required by the Office of Management and Budget](#) to adopt a “cloud-first” policy as part of the 2012 budget process.

Jeff Zients, chief performance officer and deputy director for management at OMB, [made the announcement](#) during a speech at the Northern Virginia Technology Council in Vienna, Va.

“What this means is that going forward, when evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists,” Zients said.

Zients also said OMB will help agencies with this by setting up secure, government-wide cloud computing platforms.

6. “U.S. CIO VanRoekel Outlines What's Next For Fed Tech”

Information Week, October 26, 2011

<http://www.informationweek.com/cloud/us-cio-vanroekel-outlines-whats-next-for-fed-tech/d/d-id/1100970>

Clearly the Cloud First policy was big news in 2010, which continued in 2011 when Steven Van Roekel replaced Vivek Kundra as Federal CIO, for example, in this *Information Week* article shortly after VanRoekel’s August 2011 appointment.

VanRoekel reiterated many of the goals of former CIO Vivek Kundra, whom [he replaced in August](#), including continuing to consolidate federal data centers and implementing cloud computing according to the “cloud first” mandate issued by the government earlier this year to cut costs and create efficiencies.

VanRoekel also discussed how he plans to advance Cloud First to what he calls “Future First.”



Reference Guide: Cloud / SaaS Policy Review

The federal government long has been faulted for its outdated approach to implementing technology. Although Kundra began to change that, particularly with his focus on using the cloud to replace legacy software and hardware, VanRoekel said he will take this work even further through a plan he called Future First.

"Much as our 'Cloud First' policy changed the landscape of IT spending, 'Future First' will jump start the government's adoption of new technologies and approaches," he said. "I envision a set of principles like 'XML First,' 'Web Services First,' 'Virtualize First,' and other 'Firsts' that will inform how we develop our government's systems."

Under VanRoekel's leadership, the government's goals have evolved from consolidation, efficiency and cost-cutting to ...*"better ROI, increased productivity, and improved engagement with the public."*

7. "An Interview with Federal CIO Steven VanRoekel on the Future of Computing"

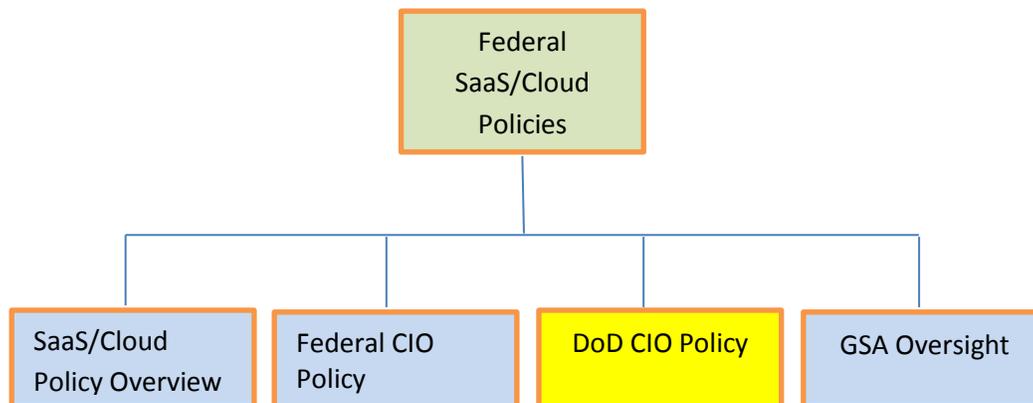
Matt McLaughlin and Jimmy Daly, *FedTech Magazine*, April 22, 2013

<http://www.fedtechmagazine.com/article/2013/04/fedtech-interview-federal-cio-steven-vanroekel>

The Cloud First policy continues to have significant impact on all technology procurements today. In this interview with FedTech Magazine, VanRoekel discusses the advances made in mobile computing and talks about addressing cyber-security concerns on a more consistent government-wide basis through the implementation of FedRAMP.



SECTION 3 DOD CIO POLICY



In the *Fierce Government IT* article extensively excerpted in Section 2 for Federal CIO policy, DoD CIO Teri Takai raised concerns and received assurances about cyber-security with Cloud First (Section 2.2.6). The DoD CIO has since published a formal, comprehensive 44-page cloud strategy document.

3.1. DoD Cloud Computing Strategy

The entire “DoD CIO Cloud Computing Strategy – July 2012” document, which includes the following sections, can be viewed at <http://www.defense.gov/news/DoDCloudComputingStrategy.pdf>.

- a. Background Information
- b. Federal Mandates Driving Cloud Adoption
- c. Program Phases
- d. Next Steps
- e. CIO Policies <http://dodcio.defense.gov/>

The strategy document states the DoD’s computing goal as follows:

Implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department’s mission, anywhere, any time, on any authorized device.



Reference Guide: Cloud / SaaS Policy Review

In order to provide a clear sense of the CIO's strategy, the opening paragraphs of the Executive Summary are reproduced here. The full document is available at the site listed above.

In the current political, economic, and technological landscape, information technology (IT) is expected to provide extensive and ever - increasing capabilities while consuming fewer resources. With the increase of both state - sponsored and independent cyber threats, the Department of Defense (DoD) is recognizing the growing importance of leading a strong and secure presence in cyberspace.

Concurrently, global financial events are driving a need for continued budgetary constraints and stricter financial oversight. As a result, the Department must transform the way in which it acquires, operates, and manages its IT in order to realize increased efficiency, effectiveness, and security. The Department has begun this transformation by establishing a set of initiatives that are aimed at achieving improved mission effectiveness and cybersecurity in a reengineered information infrastructure. The result of this new effort will be the Joint Information Environment, or JIE.

The Joint Information Environment is a robust and resilient enterprise that delivers faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location. The DoD Enterprise Cloud Environment is a key component to enable the Department to achieve JIE goals. The DoD Cloud Computing Strategy introduces an approach to move the Department from the current state of a duplicative, cumbersome, and costly set of application silos to an end state which is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs.

The DoD Chief Information Officer (CIO) is committed to accelerating the adoption of cloud computing within the Department and to providing a secure, resilient Enterprise Cloud Environment through an alignment with Department - wide IT efficiency initiatives, federal data center consolidation and cloud computing efforts. Detailed cloud computing implementation planning has been ongoing and informs the JIE projected plan of actions and milestones in Capabilities Engineering, Operation and Governance efforts.

The strategy document also lists the federal mandates driving the overall government cloud strategy as follows:

1. 2012 National Defense Authorization Act (NDAA) (PublicLaw11281):
2. Secretary of Defense (SecDef) Efficiencies Initiative



Reference Guide: Cloud / SaaS Policy Review

3. Office of Management and Budget (OMB) directed Federal Data center Consolidation Initiative (FDCCI)
4. Federal CIO 25 Point Implementation Plan to Reform Federal Information Technology Management
5. Federal Risk and Authorization Management Program (FedRAMP)
6. DoD IT Enterprise Strategy and Roadmap (ITESR)

The DOD CIO strategy program phases are listed as follows:

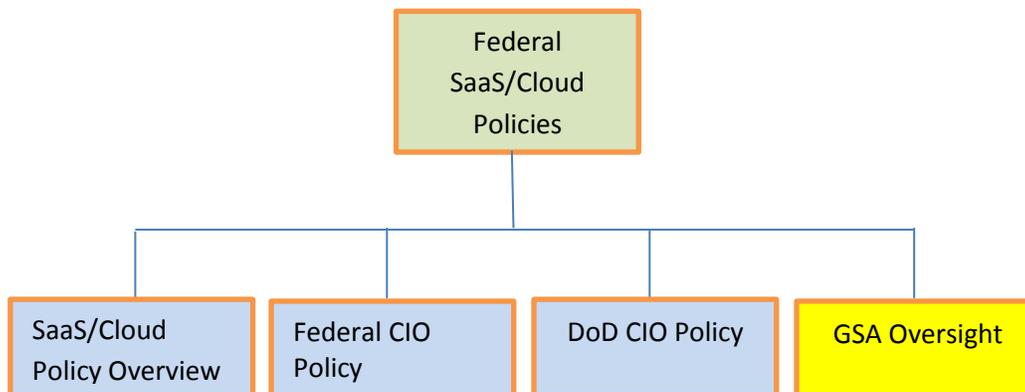
1. Foster Adoption of Cloud Computing
2. Optimize Data Center Consolidation
3. Establish the DoD Cloud Enterprise Infrastructure
4. Deliver Cloud Services

It is strongly recommended that you review the entire document for the details of the strategy phases and next steps.

Please also note the presentation in Table 1 of the document ("Cloud benefits: Efficiency, Agility, Innovation"), followed by the bullets on Reduced Costs/Increased Operational efficiencies, Increased Mission Effectiveness, and Cyber-security, and Table 2 ("Challenges Moving to a Cloud Computing Environment").



SECTION 4 GSA OVERSIGHT



GSA Oversight of cloud computing, especially the procurement and security aspects, is a broad topic which includes the FedRAMP Program, NIST and FISMA policies and procedures, the Federal Cloud Compliance Committee, and other initiatives throughout the federal government. The authoritative source for GSA cloud oversight programs is:

<http://www.gsa.gov/portal/content/190333>

4.1. GSA's Mission for Cloud Computing

The mission statement for Cloud IT Services on the GSA's website is reproduced here:

The Cloud First policy mandates that agencies take full advantage of cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost.

We help agencies comply with mandates and guidelines for moving to the cloud. Our cloud IT services provide convenient, on-demand access to a shared pool of computing resources that can be quickly and easily configured, provisioned, and released.

To help your agency move to the cloud more efficiently and better plan for developing new cloud applications, [please refer to the standardized Cloud migration statement of objectives \(SOOs\) templates below.](#)

(This entire section of the GSA website is dedicated to Cloud Guidance.)



Reference Guide: Cloud / SaaS Policy Review

4.2. FedRAMP

One of the most important tools used by GSA to oversee cloud computing is FedRAMP, which is an acronym for Federal Risk and Authorization Management Program. As the name would indicate, the focus of this program is on risk management. The primary goal of FedRAMP is stated at <http://www.gsa.gov/portal/category/102439> as follows:

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. This approach uses a “do once, use many times” framework that saves cost, time, and staff required to conduct redundant agency security assessments.

FedRAMP is the result of close collaboration with cybersecurity and cloud experts from GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council and its working groups, as well as private industry.

4.2.1 Guide to Understanding FedRAMP

A comprehensive “**Guide to Understanding FedRAMP**” (version 1.2, April 2013) is available at: http://www.gsa.gov/portal/mediaId/170599/fileName/Guide_to_Understanding_FedRAMP_042213

This document was jointly created by GSA, DHS, DoD and NIST. Its key contents are as follows:

1. Governance
2. Program goals and benefits
3. FedRAMP Process
4. Assessment application
5. Assessment process
6. Security controls
7. Joint Authorization Board (JAB)
8. Authority to Operate (ATO)
9. FedRAMP standard contract clauses

This guide provides detailed processes and procedures for security assessments including security plan recommendations.



Reference Guide: Cloud / SaaS Policy Review

4.2.2 Mandatory Program for Using Cloud Service Providers

FedRAMP is a mandatory program for the assessment, certification and use of Cloud Service Providers (CSPs). It uses internal resources on Joint Authorization Board (JAB). They perform risk authorizations and grant provisional Authority to Operate (ATO) to CSPs. Members of the JAB are the CIOs from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense.

As stated on the GSA website:

The FedRAMP assessment process involves the following key process areas: initiating, assessing, and authorizing (provisional or Agency ATO), leveraging, and ongoing assessment and authorization.

Also from the GSA website:

The FedRAMP security controls are based on NIST SP 800-53 R3 controls for low and moderate impact systems and contain controls and enhancements above the NIST baseline for low and moderate impact systems that address the unique elements of cloud computing.

The website explains the use of Third-Party Assessment Organizations (3PAOs) as follows:

CSPs that go through FedRAMP must use a 3PAO to provide an independent verification and validation of the security implementations required by FedRAMP. FedRAMP provisional authorizations must include an assessment by a FedRAMP accredited 3PAO to ensure a consistent assessment process.

4.3. GSA Recommendations for Effective Cloud Agreements

Another aspect of GSA oversight of cloud computing is the provision of information and resources for buying and implementing cloud services. One important reference available from the GSA IT Services website for cloud computing is the link for “Creating Effective Cloud Computing Contracts,” which directs the user to a document created by the CIO Council, the Chief Acquisition Officers Council and the Federal Cloud Compliance Committee (FC3).

This document, “**Creating Effective Cloud Computing Contracts for the Federal Government,**” is the authoritative resource for guidance on creating effective cloud agreements. It thoroughly discusses the following topics:

1. Selecting a Cloud Service



Reference Guide: Cloud / SaaS Policy Review

2. CSP and End -User Agreements
3. Service Level Agreements
4. CSP, Agency, and Integrator Roles and Responsibilities
5. Standards
6. Security
7. Privacy
8. E-Discovery
9. Freedom of Information Act
10. Federal E-Records Management

Appendix A of the document includes a series of important questions that the procurement professional should use to guide the creation of a comprehensive cloud agreement.

4.4. GSA’s Cloud Migration SOO Templates

Another important resource provided by GSA is a series of migration Statement of Objectives (SOO) templates, which are designed to guide the migration process from legacy systems to cloud services.

The following is taken from the GSA cloud services website:

GSA's Multi-Agency Working Group developed the sample SOOs below. Agencies will realize cost savings quicker through increased efficiency, agility, and innovation, and will require less time to close data centers.

The sample SOO templates support two key administration priorities — Cloud First and data center consolidation.

Cloud Migration Phase	Cloud Sample SOO Templates	File Type/Size
1. Inventory 2. Application Mapping 3. Migration Planning	Cloud Migration Services SOO template phases 1 - 3	Word, 42 KB
4. Migration Execution	Cloud Migration Services SOO template phase 4	Word, 41 KB



Reference Guide: Cloud / SaaS Policy Review

5. Decommissioning Services, Equipment Disposition, and Facility Disposition	Cloud Migration Services SOO template phase 5	Word, 40 KB
Instructions	Instructions/executive summary for SOO template phases 1 - 5	Word, 27 KB

4.5. Additional Resources

The following websites provide additional insights into the roles of GSA, NIST and other groups in assisting federal agencies to take advantage of cloud benefits as fast and cost effectively as possible.

1. CIO.gov – Cybersecurity and FedRAMP
 - a. <https://cio.gov/cyber-security-2/fedramp/>
2. FedRAMP, NIST and FISMA – Integrated Cloud Policies & Procedures
 - a. <http://www.nist.gov/itl/cloud/index.cfm>
 - b. NIST 800-53 SP Revision 3 catalog of controls
 - c. NIST Computer Security Division – Implementation of Federal Information Security Act of 2002 (FISMA)
3. Other GSA and Federal Cloud Initiatives
 - a. [Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies](#)
 - b. [The Federal Cloud Computing Initiative](#) <http://info.apps.gov/node/2>
 - c. [A Report on Federal Web 2.0 Use and Record Value](#) <http://www.archives.gov/records-mgmt/resources/web2.0-use.pdf>
 - d. [NIST Computer Security Resource Center - Cloud Computing](#) <http://www.nist.gov/itl/cloud/>
 - e. [Guidance on Managing Records in Cloud Computing Environments](#) <http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html>