Volume 3 Number 4 June 2011

ON THE FrontLines

Government Cloud Computing

The Federal Cloud Computing Strategy Is Unleashing The Power Of Cloud.

ON THE FrontLines MEDIA GROUP

TREZZA Media Group Connecting Partners Through Mindshare Media

Public Sector COMMUNICATIONS

the Flyzik group

By Jeff Erlichman, Editor, On The FrontLines

Unleashing The Power of Cloud

With a cloud computing approach, a cloud customer can spend less time managing complex IT resources and more time investing in core mission work.

Think "Cloud First" first!

"To harness the benefits of cloud computing, we have instituted a Cloud First policy," wrote Federal CIO Vivek Kundra in the Federal Cloud Computing Strategy.

Over time, this strategy — if fully implemented — will fundamentally change the way government approaches, uses and buys computing infrastructure and resources.

Cloud computing offers the government an opportunity to be more efficient, agile, and innovative through more effective use of IT investments, and by applying innovations developed in the private sector asserts Kundra.

"If an agency wants to launch a new innovative program, it can quickly do so by leveraging cloud infrastructure without having to acquire significant hardware, lowering both time and cost barriers to deployment."

The rapid progression from the Federal Data Center Consolidation Initiative (FDCCI) to the 25 Point Implementation Plan to Reform Federal IT Management to the Federal Cloud Computing Strategy demonstrates the desire to accelerate the government's migration to cloud based services and save budget dollars.

"This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments."

So, the debate is over for Federal program and IT managers. It's "Cloud First" first.

2012 Cloud Deadlines

Consistent with the Cloud First policy, "each agency will reevaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process."

OMB has given Federal managers concrete deadlines to move computing resources to the cloud:

- **February 2011** — Cloud First Strategy Published
- **May 2011** — Three "must move" services identified for migration to the Cloud
- **May 2012** — First "must move" service migrated to the Cloud
- **November 2012** — "Must move" services 2 & 3 migrated.

These actions collectively will save taxpayers billions — with a "B" — of dollars in heating, cooling and computing energy and power costs.

"The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints," Kundra declares.

Now, it is on the shoulders of both government and the private sector (whose must really deliver on their promises) to unleash the power of the cloud for government. ■

$20 Billion For Cloud In 2012?

In 2012, an estimated $20 billion of the Federal Government's $80 billion in IT spending is a potential target for migration to cloud computing solutions estimates the Federal Cloud Computing Strategy.

In agency estimates reported to OMB, the following agencies could spend more than $2 billion: DHS, Treasury, DOD, VA, DOT and Commerce. HHS, State and Energy could each top $1 billion in 2012.

According to Federal CIO Vivek Kundra, "cloud computing describes a broad movement to treat IT services as a commodity with the ability to dynamically increase or decrease capacity to match usage needs.

By leveraging shared infrastructure and economies of scale, cloud computing presents Federal leadership with a compelling business model. It allows users to control the com puting services they access, while sharing the investment in the underlying IT resources among consumers.

Users pay for what they consume, can increase or de crease their usage, and leverage the shared underlying resources. Cloud computing enables IT systems to be scalable and elastic; end users do not need to determine their exact computing resource requirements upfront.

Instead, they provision computing resources as required, on-demand. Using cloud computing services, a Federal agency does not need to own data center infrastructure to launch a capability that serves millions of users."

Source: Federal Cloud Computing Strategy, Vivek Kundra, Federal CIO, February 8, 2011

Inside Unleashing The Power of Cloud

ON THE FrontLines MEDIA GROUP
TREZZA Media Group
Public Sector Communications
the Flyzik group

Change is good. You First!

Dr. David McClure (GSA), Pete Tseronis (DOE) and David Mihelcic (DISA) are three leaders of the government charge to unleash the power of cloud.

"Cloud First" mandates are fine, but you need dedicated people to make it actually happen.

While 64% of Federal CIOs plan to move to Cloud First in the next two years, 79% are not using the mandated policy today, according to the 2011 Federal Cloud Weather Report survey from MeriTalk.

Further the study reaffirms the fact that most agencies are still in the initial stages of cloud implementation with only 17% maintaining IaaS; 15% SaaS and 13% PaaS. So, while CIOs know they must adopt change, clearly they first want to look for success stories and templates they can apply.

Three of those leaders instrumental in helping agencies unleash the power of cloud in government talked about their efforts during the recent **Federal Executive Forum**:

- **Dr. David McClure**
  Associate Administrator of the Office of Citizen Services and Innovative Technologies, GSA
- **Pete Tseronis**
  Chief Technology Officer, Energy
- **David M. Mihelcic**
  Chief Technology Officer, DISA

Free To Focus On Mission

Dr. McClure runs the Cloud PMO, whose role is to be a catalyst for using cloud to deliver common services across government.

The PMO is working on several fronts: with FAS to open procurement vehicles conducive to cloud services (more on page 12); and with the White House on FedRAMP which will provide a governmentwide common cloud security framework (more on page 8).

"What FedRAMP is trying to do is simplify the security process for the government," he explained.

The way it operates now is compliance focused and a vendor has to go agency by agency by agency and get security authorizations to operate. Changing that allows the leveraging of these accreditations and certifications across agencies.

"We can do it 4x faster at ½ the cost of what we are spending right now," noted McClure.

Simplicity, speed, agility and reduced costs are real tangible benefits said McClure, but "I think the real benefit we are seeing is that is does release your attention away from technology to mission improvement, performance and results."

Federal Cloud Computing Advisory Council

In addition to his day job as CTO leading cloud efforts at DOE, **Pete Tseronis** is co-chair of the Federal Cloud Computing Advisory Council. The CCAC serves as a collaborative environment for senior IT experts from across the federal government.

"Cloud is forcing everyone to rethink a lot of things; what do we move, what do we keep," said Tseronis who asserted cloud be viewed as an opportunity to change the culture for the better.

"It gives us a chance to step back from our entrenched solutions and have a meaningful and hopefully quantifiable discussion about how much is a service is worth," explained Tseronis.

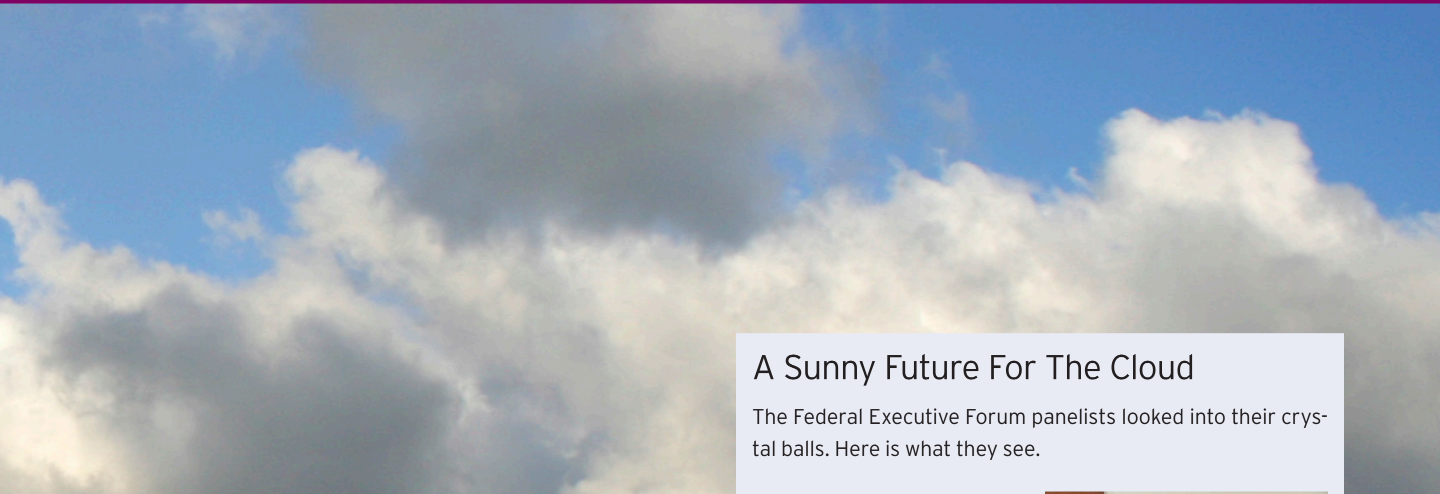
"What is the risk reward ratio? In house vs. outsource? Is there is an alternative to the old way of doing business? Information doesn't have to be locked in a file anymore; it is open to comment on a wiki or blog. With cloud people have to do something different from what they are used to doing." In other words, while change is good, the "you first" mindset still is at work.

Implementing On Demand Infrastructure

"I think of cloud as doing for computing as what IP did for networking," exclaimed DISA CTO **David Mihelcic** which is the cloud provider for DoD.

"Today we are putting in place an infrastructure to provide on demand saleable cloud services at multiple class levels so DoD program managers can put their apps in the cloud and make it easier for the end users to derive service," said Mihelcic.

Programs in progress include RACE for web provisioning, Forge.mil for collaboration and the Army enterprise email rollout. What these programs do is bring speed and agility to an environment where a typical DoD big software program might deliver a



software release every 6-18 months.

"Leading edge companies who deliver services on the Internet (e.g. Flickr) have on average 10 releases of software a day. That is where we need to move with cloud. We need to rapidly develop, test, integrate and push to production and then rapidly scale that."

Mihelcic said DISA is actively focusing on doing away with stovepipes and silos. "If you have a legacy app that serves a small organization and you move that to the cloud, and it remains a stovepipe in the cloud, then you really haven't changed things," he said. "What we are seeking to do is promote capabilities from locally relevant to globally relevant so they can serve our entire enterprise."

"One of the keys in doing security is having a standard database of identity for everyone in our enterprise and have standard methods of authentication of access," he said. By having role based authentication, "we break down many of the barriers to information sharing."

Dynamic Management Approach

We have challenges, but challenges are good for forcing change and good for forcing innovation according to McClure.

"Cloud changes the ball game for industry and government in terms of services and pricing," said McClure. "It is a different pricing model than we are used to dealing with," explaining that pricing on demand flexibility and scalability is not just a government problem, it is a provider problem as well. Plus CIOs will have to decide whether they are going to be cloud consumers or cloud providers.

"This is the year of moving to cloud, to stop debating models and concepts and have some real services on the cloud," added McClure.

"It is a challenge for CIOs to manage in a hybrid cloud, non-cloud environment. At GSA we are looking for vendors that have very dynamic management approaches to really optimize the IT performance that is both cloud based and non-based, because we won't move everything to the cloud." ■

A Sunny Future For The Cloud

The Federal Executive Forum panelists looked into their crystal balls. Here is what they see.

Dr. David McClure
Associate Administrator of
the Office of Citizen Services
and Innovative Technologies
GSA

"The future is going to be a trusted consumer based computing model...most of time in government we hear from IT shops why things can't be done fast, easy, and conveniently, that model is going out the door...we are moving into an environment where as a consumer I should be able to select, provision and manage a solution in days or weeks... that is a game changing orientation in the way govt. buys, procures, uses and manages IT..."

Pete Tseronis
Chief Technology Officer
Energy

"I see less dollars to the infrastructure because of cloud opportunities...I see GSA vehicles becoming that open source for procurement...all the great work that is being negotiated upfront; agencies need to take advantage of what GSA is doing...in five years if we are not doing that, we are doing a disservice to taxpayers for not taking advantage of those cost savings..."

David Mihelcic
Chief Technology Officer
DISA

"The DoD warfighter will be able to go anywhere in the world and from any device, access the information they need to accomplish their mission...I want a warfighter to be able to walk up to any machine, insert their ID card and access their network; be able to reach into the cloud and pull their apps off the cloud and data out of the cloud and be able to ubiquitously share data with anyone they need to..."

Cloud Proving Grounds

Email and collaboration applications at DHS, GSA and USDA
are proving the benefits of service provisioning over asset ownership.

The strategy is meant to be disruptive.

"Where we are heading — and we have sent a very clear signal from a demand perspective — is that we want the federal government to move away from the old model of IT management and IT acquisition, which was based around asset ownership, and shift to service provisioning," Federal CIO **Vivek Kundra** told the audience during a panel at a recent AFCEA Bethesda breakfast.

"We want to make sure that the shift is disruptive in nature," asserted Kundra.

As a concrete example, he told the audience how his office had halted about $20 billion worth of financial systems and literally decided to terminate a number of those systems after spending billions on systems that were underperforming. "We decided to descope significantly by billions of dollars a lot of these ERP systems that were in play."

"So as we look at agencies like the Consumer Financial Protection Bureau, we are trying to think of how do you actually build a brand new agency with zero asset ownership? No need to own a data center, no need to actually go out there and buy these complicated IT systems. That is the idea that we are driving towards."

That may be the future, but shifting away from asset ownership is already saving millions for GSA and USDA who have shifted their email to the cloud.

"They don't need to own dozens to thousands of servers to operate something as simple as email," Kundra explained. "What is even more shocking is that on something as simple as email, GSA has been able to save over $6 million and USDA was able to save over $15 million, and the numbers keep going up. Imagine what would happen if we went after the financial systems?"

Budget Haircut To Private Cloud

No matter how strategic the agency, IT is taking a "budget haircut" governmentwide. That includes DHS CIO **Richard Spires** told the audience.

"We are going to be about $400 million less," announced Spires. "We have the same challenge: to greater use and leverage commodity IT, because every dollar that we can free up by doing commodity IT better, enables us to deliver more mission effectiveness."

While DHS is currently reducing the number of enterprise data centers from 24 down to those 2, they are not stopping there according to Spires.

"We are really setting up our own private cloud capability within those two data centers. And just awarded recently both email as a service capability within our own private cloud," Spires said. "Because of the security reasons and the sensitivity of our data, we didn't yet feel comfortable going out to the public cloud."

Federal CIO Vivek Kundra presents case examples to illustrate the cloud framework in the Federal Cloud Strategy.

"We have scale. Eventually we should scale this to well over 200,000 mailboxes. We already have headquarters, FEMA and CBP signed up and that gives us right around the 100,000 mail boxes. Starting this fiscal year we should finish headquarters this fiscal year, finish hopefully FEMA and CBP early next fiscal year and that migration. That there is 100,000, so we have got the scale to be able to drive that kind of pricing within our own private cloud," Spires explained.

DHS also awarded SharePoint as a service in another set of private cloud offerings said Spires. "We are standing up development and test in order to be able to get out of the business of you start a new project program and all of a sudden you've got to stand up a new development and test environment."

$20 Billion To The Cloud

While Kundra points to the success of early adopters at GSA, USDA, Defense, DHS, VA and HHS, he clearly recognizes that the market is far from mature.

"All the solutions don't exist. One of the things I challenged the private sector on was to make sure that they are standing up a secure solution so that the government could move to the cloud in a safe, secure manner."

In fact Kundra says from an agency perspective, from a demand perspective, his office has been able to identify about $20 billion worth of IT systems that could move to the cloud in FY2012 in the right conditions.

While early cloud adoption is revolving around email and collaboration, Kundra said there is much interest in infrastructure solutions that dovetail with service offerings (IaaS, SaaS and PaaS) including information security. Agencies are interested in figuring out how do they provision security as a service rather than hire all of these people "because you are constantly racing to the bottom and you can't really keep up," added Kundra.

"So I think you are going to see a philosophical shift from asset ownership to service provisioning, which would be one of the megatrends that I would point out in the coming year — and especially in 2012." ■

Fast Tracking FedRAMP

FedRAMP — the Federal Risk and Authorization Management Program — is being established to provide a standard approach to Assessing and Authorizing (A&A) the security of cloud computing services and products.

Secure or not secure?

For agency leaders, that fundamental question about the cloud needs to be answered "YES". More than that, whatever cloud provider chosen must be assessed and authorized to provide cloud computing services and products to the government.

Speeding Cloud Procurements

So, while the cloud provides agility, it also presents a challenge for agency IT to get the security piece "right" — and do in a way that is quick and easy to understand.

"What we are trying to do with the FedRAMP processes is bring some efficiencies to how we do this in the federal government," explained Dr. David McClure, GSA Associate Administrator Office of Citizen Services and Innovative Technologies at a recent Federal Executive Forum.

"If you are moving to the cloud environment, you want to be able to move in it quickly. And as it turns out, the way we are doing a lot of the security authorizations, and security assessments and accreditations is agency by agency.

Approve Once, Use Often

Dr. David McClure

GSA

"We are trying to shorten the acquisition process...the next question is has it been authorized through FISMA?..."

Doing that is costly said McClure. An average authorization and assessment (A&A) costs up to $180,000 and requires up to six months to complete. FedRAMP allows joint authorizations and continuous security monitoring services for government and commercial cloud computing systems.

"Joint authorization of cloud providers results in a common security risk model that can be leveraged across the federal government," explained McClure.

"A common security risk model is also a consistent baseline for cloud based technologies ensuring that the benefits of cloud-based technologies are effectively integrated across the various cloud computing solutions. The risk model enables the government to 'approve once, and use often'", explained McClure.

"We are trying to shorten the acquisition process," said McClure. "If I go onto GSA Schedule or a BPA to choose a cloud solution, the very next question that has to be answered is: Has it been authorized for use in the government through the FISMA process? If it hasn't it can take anywhere from 30 days to 3-6 months."

FedRAMP creates a process where the assessment and accreditation is done based upon existing criteria that is agreed upon and through a fundamental process that is transparent said McClure.

"It increases the trust around the government that that accreditation was done by the standards the government has agreed to; and that it was done with a great deal of soundness so that it can be reused by other entities rather than duplicated or repeated agency by agency."

For information on FedRAMP status, click here. ■

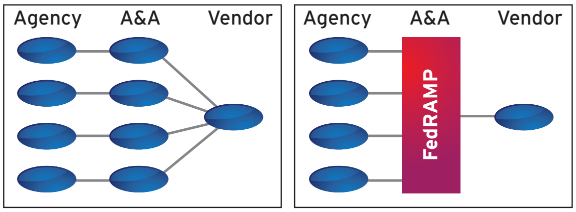
Why Fast Track FedRAMP?

As FedRAMP allows agencies to reuse authorizations, participating agencies need only review security details and leverage the existing authorization in order to secure agency usage of the candidate system. This should greatly reduce cost, enable rapid acquisition, and reduce overall level of effort by both government and industry technology providers.

FedRAMP's processes, policy implications, governance, and technical security standards have all been arrived at via a consensus-based approach within government with NIST, DHS, DoD, NSA, numerous industry consortia, and many other federal and state and local government entities have all collaborated with GSA to arrive at the current state.

Source: GSA

Details of Federal Risk and Authorization Management Program (FedRAMP)



Before

- Duplicative risk management efforts
- Incompatible requirements
- Potential for inconsistent application & interpretation of Federal security requirements
- Redundant agency security certification costs

After

- Unified Risk management & associated cost savings
- Inter-Agency vetted and compatible requirements using a shared cloud service
- Effective & consistent assessment of cloud services

OTFL Interview

Alan Lewis

Vice Director, Computing Services, Defense Information Systems Agency (DISA)

The Vice Director describes DISA Cloud Services activities in this interview with OTFL.

OTFL: Can you give a brief overview of DISA Cloud services?

Alan Lewis, DISA: We operate a DoD Community Cloud, that provides a global content delivery service with distributed management and rapid continuity of operations and restoral capability between data centers.

Further, we have a new contracting model that we've embraced that provide our 'infrastructure enablers' as commodity services. Examples of that are: infrastructure capacity-as-a- service (CaaS) in terms of the processor operating environment; platform-as-a-service (PaaS) in terms of the web hosting environment; and storage-as-a-service.

Our focus right now is becoming the DOD provider for joint enterprise services. Our first large scale implementation across the Department is enterprise email and the first adopter is the Army.

Now in order to do that, (we look) for common enterprise service infrastructure enablers. For example, enterprise email is supported by the Identity Synchronization Service (IdSS) that provides a single authentication source as well as a global active directory (AD) capability.

IdSS and AD will also support enterprise SharePoint providing a common underpinning to reduce overall costs.

OTFL: What advice would you offer civilian customers about migrating to the Cloud?

Alan Lewis, DISA: The cloud environment significantly improves performance reliability and scalability. Our observation is that it significantly improves the end user experience. The associated challenge is that there are significant complexities to establish all of the required foundational elements.

In that sense a provider has to account for multiple aspects ranging from the ability to dynamically and rapidly scale all aspects of the service, including the virtual operating environments, the ability to rapidly provision additional terabytes of storage, and our business and management processes. We refer to our operational processes as tactics, techniques and procedures or TTPs.

In addition you need clear governance and well defined roles and responsibilities to effectively manage all of the multiple interdependencies. Another key requirement is to maintain effective configuration control and what we call 'hyper or brutal standardization'. We must also simplify our business processes and ensure that they are clearly understood by our customers.

The distributed management of the servers, operating systems, databases, communications and other infrastructure elements requires awareness of what customer capabilities are hosted on any given server operating environment (OE) as well as the operational implications of an outage and restoral priorities.

In that sense, even with scheduled outages such as our scheduled service interruptions, we need to know: what are the implications of that interruption to all users that might be impacted, including first order effects as well as second and third order effects.

So what that requires is clearly defined roles, responsibilities and authorities for any required actions. One example of a key action is when to COOP a given capability. Again, I mentioned the standardization and that's really more than standardization of hardware and operating systems, (it's the) operational environment and standardization of our business and operational processes, including our service level agreements.

OTFL: You used the word brutal. Were you using the word brutal in the way that most people would?

Alan Lewis, DISA: I heard a much gentler term and that is hyper standardization. It really is the key because everything stems from employing standardization across the board. Every aspect of our infrastructure and operations should be standardized.

Now that doesn't mean that you only do it my way.

It means that we provide an environment that supports a full range of capabilities that are needed and a full range of storage solutions, but we must settle on a subset of the many commercially available systems to provide these capabilities.

We have to move away from a heterogeneous environment to one that is as homogeneous as possible, at least within those subsets that we offer.

Because the cost drivers are there; for example, every new system we field has a dedicated trained set of personnel, not just on our side but through the different tiers or levels of help desks. The more operating systems supported, the more database solutions supported, the more labor is required, and frankly our largest costs are associated with labor.

OTFL: How can the Cloud speed up the delivery of content for the Warfighter?

Alan Lewis, DISA: The heart of our mission is to serve the Warfighter. The cloud can be used to speed up the delivery of content. There are several ways to do it.

One is that we strategically host capabilities in regionally located Defense Enterprise Computing Centers (DECCs).

We look at in terms of where the capability itself and the operating environment are located. We also look at where the Service Desk is located, because there are some benefits there in terms of being located in the same time zone from a Service Desk perspective. Proximity is always good, even though we know electrons travel at the speed of light, what we have found is where we can geographically position ourselves we do.

The other aspect is that we forward stage critically and repeatedly accessed data. We do that through our Global Content Delivery Service (GCDS). This reduces the amount of bandwidth that's required as well as significantly speeds information delivery to the end user. From an infrastructure provider standpoint, it significantly cuts down on the repetition of high bandwidth or bandwidth intensive applications data and data files by positioning those forward.

From a user performance standpoint significantly, in some cases we have order of magnitude measured improvements in speed of delivery and reduced latency, especially our forward deployed users accessing critical data.

OTFL: Can you provide an update on the migration of email? Where do you stand right now?

Alan Lewis, DISA: As I'm sure you are aware, this is probably our most visible Departmental enterprise service initiative and will be the largest scale joint enterprise capability that DISA has implemented; with an expectation that it will grow to serve the entire Department of Defense.

So where we are is we've completed key foundational elements such as the identity synchronization service, as well as our active directory enterprise application service that provides the directories and can scale to serve the four million plus users in DoD.

We have begun user migrations And by December 31 we will complete migrations for all Army units, the European Command, the Africa Command and the US Transportation Command.

OTFL: You've described what you are doing for the Army; what are your plans with the other services?

Alan Lewis, DISA: We are actively moving ahead with all the Services; for example with the Air Force, we have already migrated a significant amount of their personnel services web portal capabilities. This will support the Air Force as they move to centralize all of their personnel services via a single access platform.

This will provide services that include active duty and Air Force reserves as well as the civilian work force and retirees. It's a 24x7 total force personnel service to increase performance and reliability and decrease web page loading times.

With this migration, we are also providing the Air Force additional cost savings because they will be leveraging existing DISA infrastructure services contracts rather than supporting new development or replacement of in-house web servers across the service.

The Air Force Personnel Command and the Air Reserve Personnel Center are the first components to move their knowledge bases over to a DISA hosted environment as part of this effort.

OTFL: Can you talk about your consolidation efforts with the Air Force Global Broadcast Service and the Navy?

Alan Lewis, DISA: The Air Force Global Broadcast Service (GBS) is the real time dissemination of information to the deployed users using satellites and sophisticated broadcast management facilities.

To provide secure real time streaming video and file transfers to and from remote deployed users, GBS has built on the successful DISA Digital Video Broadcast – Return Channel Satellite (DVB-RCS) capability to implement a two way capability. Key savings for the Air Force will be realized by migrating multiple regional Satellite Broadcast Management (SBM) facilities from CONUS and Hawaii to a DECC.

The new system hosted in a DECC will achieve significant cost reductions in staff and facility operating costs, improve reliability and provide increased automation for more rapid response to operational needs.

With Naval Sea Systems Command, we are consolidating their SharePoint portal. What we are doing there is migrating and updating their existing 2007 SharePoint portals from Microsoft 2007 to SharePoint 2010 and hosting in our DECC environment.

We are also adding new capabilities, such as COOP. By consolidating multiple NAVSEA SharePoint portals to a single instance, there's going to associated cost savings, as well as the ability to provide some extranet capabilities. This is a great example of where we are partnering with the Navy to decrease their costs and increase availability of a capability by employing a DECC hosted redundant architecture.

OTFL: Can you talk about the Rapid Access Compute Environment (RACE)? It's undergone some enhancements since its launch, hasn't it?

Alan Lewis, DISA: It sure has. The original focus for RACE was on the development and test environment and to provide our Department of Defense customers the ability to acquire that development and test environment in 24 hours.

We have now implemented a methodology that supports security accreditation for new applications. This will enable and accelerate the path to production from the development and test environment.

Specifically, we are offering tools that will help RACE users organize and consolidate all the required security documentation. We also now support an accreditation model where the users that conform to the RACE baseline will inherit the security controls in the baseline as well as the DECC infrastructure controls. That also will aid them in a more rapid move to a production environment.

By linking RACE with the tremendous capability provided by Forge.mil on the software side, DISA provides a full solution environment that couples the processing and memory environment in RACE with the powerful application development environment of Forge.mil. ■

Cloud Shopping Made Easy

GSA Infrastructure and Email as-a-service BPAs promise to give buyers access to secure cloud-based solutions to meet 2012 cloud migration deadlines.

Speed, simplicity and customer orientation are watchwords you often hear in the commercial world. Now they are the watchwords of government as well.

Dr. David McClure
GSA

"Agility is now the watchword for technology," declared GSA's Dr. David McClure during a recent Federal Executive Forum.

Through the Cloud PMO, GSA has taken the the lead in facilitating new innovative cloud computing procurement options; ensuring effective cloud security and standards are in place; and identifying potential multi-agency or government-wide uses of cloud computing solutions, McClure said.

GSA is also the information "hub" for cloud use examples and case studies, decisional and implementation best practices, and for sharing exposed risks and lessons learned.

"We have also established a "cloud storefront" (www.apps.gov) as a site for agencies to directly purchase cloud services," said McClure. He pointed to www.info.apps.gov "as an evolving knowledge repository for all government agencies to use and to contribute their expertise."

"We are increasingly looking at lightweight technologies; we are looking at no cost solutions; we are looking at open source," noted McClure. "We are looking a lot at the ability to move quickly to solution sets that get us customer value and get us mission value."

"That creates a completely different environment for us. It presents great opportunities, but it also presents us with extreme challenges that we have to move fast, and we have to move with confidence in order to work in that kind of environment."

McClure and his GSA Cloud PMO team realize that migrating to a services-based model means at some point you have to actually buy services. They are ready.

IaaS BPA Provide Flexibility In Purchasing

Infrastructure-as-service (IaaS) is one area where GSA is creating a Blanket Purchase Agreement (BPA) to provide quicker access to cloud solutions according to McClure.

"We awarded at the end of 2010 an infrastructure BPA to 12 vendors in this space. This is moving to the adoption of buying cloud provisioning as a commodity, as a pure commodity. I need some storage. I want to virtualize my data center. It's very simple, it's very fast, it's very easy to provision, to scale up and has incredible pricing because of the way GSA negotiated the contract," said McClure

The BPA streamlines the procurement and vetting process to allow agencies to implement solutions more quickly. Plus, all these solutions will be secure since all 12 vendors have gone through the FISMA accreditation process as well by GSA. Many have multiple partners and offer storage, computing power and website hosting as commodities.

The IaaS BPA offers federal customers a wealth of benefits, including:

- Commodity
- Standardized requirements
- Comprehensive services from a single task order
- Acquisition oversight.

Cloud Email RFQ Issued

On May 11, 2011 GSA released a request for quotation (RFQ) to provide government agencies with access to secure, cost-efficient cloud-based email solutions.

"The RFQ is for the first of GSA's Integrated Email as a Service (EaaS) cloud offerings, designed to increase the speed of agency adoption, deployment, and implementation of cloud technology," the agency said in its press release.

The Federal Computing Cloud Initiative (FCCI) is partnering with GSA SmartBUY and the DoD Enterprise Software Initiative to deliver Email-as-a-Service (EaaS) acquisition capabilities via enterprise wide BPAs says the RFQ.

The objective of this RFQ is to offer five key service offerings through EaaS providers for ordering activities.

- Lot 1: Email-as-a-Service
- Lot 2: Office Automation
- Lot 3: Electronic Record Management
- Lot 4: Migration Services
- Lot 5: Integration Services

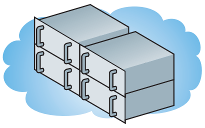
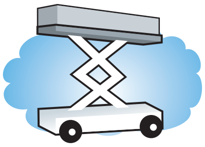
The RFQ states the total maximum quantity of all supplies and services under the Blanket Purchase Agreement (for all awardees combined) shall not exceed $2.5 billion, including the Options. The cost of awarding, administering and managing this BPA is included in the prices delineated in Section B of this BPA. The ACT fee for this Email as a Service BPA is 2%. This ACT fee is in addition to the IT Schedule 70 Fee.

Under the RFQ, GSA wants vendors to provide any, some or all of the services in four categories of cloud computing:

- Government community cloud
- Provider furnished equipment private cloud
- Secret enclave
- Public cloud

The primary activities within the Federal Cloud PMO

Promoting adoption and removing obstacles in the government-wide acquisition and utilization of cost effective, green and sustainable Federal cloud computing solutions.

Apps.gov	FedRAMP	Federal Date Center Consolidation Initiative	Infrastructure-as-a-Service	Software-as-a-Service Email	Platform-as-a-Service (Geospatial)
	FedRAMP	FDCCI			
1st Federal storefront offering commoditized cloud services	"Authorize Once, Use Many" approach to security for Cloud Service Providers	Assist agencies to consulidate at least 800 data centers by FY15	Commodity computing resources made available through GSA Blanket Purchase Agrement (BPA)	Cloud Email to be made available (Summer 2011) through BPA	Geospatial PaaS work currently underway

Source: GSA

GSA detailed mandatory requirements such as five gigabytes of storage to mobile device capabilities and e-discovery capabilities.

Lots Of Collaboration, Lots Of Interest

McClure said it will be several months before the email-as-a-service and other offerings under the BPA are up and running.

The email Blanket Purchase Agreement (BPA) is the product of the Email-as-a- Service (EaaS) Working Group efforts and brought together email and collaboration experts from across government said McClure. They took a collaborative approach to procurement by drafting requirements with input from its members leading to a cooperative procurement that will best address the needs of the federal enterprise as a whole.

"Every major provider in the space has expressed interest in being on this contract. This is not a one size fits all," asserted McClure.

"If I want a secure cloud email solution, that will be provided; if I want a wide open public solution, it'll also be provided. There are many varieties of cloud email that this will allow a government agency to decide what to choose from," said McClure.

"All again have to meet security authorization, accreditation and ATO. This will help tremendously and as you can see there's significant cost savings that are often associated with moving to a cloud based solution."

"The BPA will drastically reduce the amount of time and resources needed to procure the cloud email solution that best fits their agency's needs."

Based on Forrester Research, McClure said "an agency that leverages the BPA will be $11/mailbox/month, $1 million in annual savings for every 7,500 users, or approximately 44% over existing on-premise email solutions."

"The BPA will also accommodate a range of email services in public, private, and highly secured clouds, making robust, feature-rich, secure email and collaboration service options," noted McClure. They are similar to those currently being implemented at GSA and USDA available to any interested federal or state and local agency ."

Innovative, Economical, Efficient

McClure noted that the idea behind embracing cloud computing is not a matter of being "cool", but because it is fundamentally sound business.

"We are looking for innovative ways in which technology can be made available to us in a way that produces economies and efficiencies. It primarily does that by allowing us to go to a supply and demand model.

We use what we need, we buy when we want, and we drop what we don't need. It's a very different operating environment than what we normally have done in the federal government end user," added McClure.

"This is a dramatic shift in the computing environment; actually having information and visualization tools on your laptop, phone providing minute-by-minute updates on the information you want."

McClure acknowledges cloud is not a solution for every computing environments.

"Some computing in government is very stable. Other environments are very volatile and do scale up quickly. These are areas that are very ripe for the model of cloud." ■

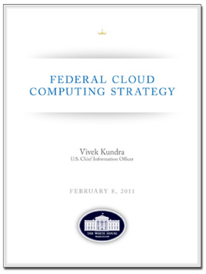
Presented by

Resources

Find more resources at www.onthefrontlines.net/cloud.

From The Federal Cloud Computing Strategy Appendix

General



FEDERAL CLOUD COMPUTING STRATEGY

Vivek Kundra
U.S. Chief Information Officer

FEBRUARY 8, 2011

The ABCs of Cloud Computing: GSA

A comprehensive cloud computing portal where agencies can get information on: procurement, security, best practices, case studies and technical resources. Link

Cloud Computing Migration Framework: Mitre

A series of technical white papers on cloud computing, including a decision-making framework, cost/business case considerations, service level agreement provisions, information security, a PaaS analysis and a survey of market segments and cloud products categories. Link

Successful Case Studies: CIO Council

This report details 30 illustrative cloud computing case studies at the Federal, state and local government levels. Link

Cloud Computing Definition: NIST

Includes essential characteristics as well as service and deployment models. Link

Security

FedRAMP – Centralized Cloud Computing Assessment and Authorization

The Federal Risk and Authorization Management Program (FedRAMP) has been established to provide a standard, centralized approach to assessing and authorizing cloud computing services and products. FedRAMP will permit joint authorizations and continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use. It will enable the government to buy a cloud solution once, but use it many times. Link

Primer on Cloud Computing Security: DHS

A white paper that seeks to clarify the variations of cloud services and examine the current and near-term poten tial for Federal cloud computing from a cybersecurity perspective. Link

Privacy Recommendations for Cloud Computing: CIO Council

A paper which highlights potential privacy risks agencies should consider as they migrate to cloud computing. Link

Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach: NIST

Link

Guidelines on Security and Privacy in Public Cloud Computing: NIST

This draft publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when out sourcing data, applications, and infrastructure to a public cloud environment. Link

Acquisition/Procurement

Cloud Computing Procurement Assistance: GSA

Apps.gov is an online cloud computing (SaaS, IaaS, PaaS) storefront that encourages and enable the adoption of cloud computing solutions across the Federal Government. Apps.gov offers a comprehensive set of business, infrastruc ture, productivity and social media applications. It eliminates unnecessary research, analysis and redundant approvals, requisitions and service level agreements across the government by providing agencies a fast, easy way to buy the tools they need. Link

Standards

Federal Cloud Computing Collaboration Page: NIST

The National Institute of Standards and Technology (NIST) has been designated by the Federal CIO to accelerate the Federal Government's secure adoption of cloud computing by leading efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders. This site provides an avenue for interested stakeholders to collaborate with NIST in developing interoperability, portability and security standards, busi ness and technical use cases, and a cloud computing reference architecture and taxonomy. Link

Technical Resources

CIO Council Executive Cloud Computing Executive Steering Committee (CCESC)

The CCESC was established by the Federal CIO Council to provide strategic direction and over sight for the Federal Cloud Computing Initiative. Under the CCESC, there exists a Cloud Computing Advisory Council and multiple working groups that further enable the adoption of cloud computing across the government. (Chaired by USAID). Link

CIO Council Cloud Computing Advisory Council (CCAC)

The CCAC was established at the behest of the CCESC to serve as a collaborative environment for senior IT experts from across the Federal Government. CCAC members serve as agency resources best practices dissemination, consensus building for key Federal Cloud Computing initiatives, and the sharing of existing/planned cloud computing projects. (Chaired by USAID). Link

CIO Council Cloud Computing E-mail Working Group

The E-mail Working Group will be the source of SaaS email information, solutions, and processes that foster adoption of SaaS email across the Federal Government. (Chaired by DOI). Link

CIO Council Cloud Computing Security Working Group

The Security Working Group sup ports FedRAMP, a centralized cloud computing assessment and authorization body that can be leveraged by multiple agencies. (Chaired by GSA). Link

CIO Council Cloud Computing Standards Working Group

The Standards Working Group will lead government-wide efforts to define cloud computing security, portability and interoperability standards, target Federal business and technical use cases, and a reference architecture. (Chaired by NIST). Link

Additional workgroups will be stood up by the CIO Council as the work of the Federal Cloud Computing Initiative evolves.

The Benefits of Cloud Computing

	Current Environment	Cloud Benefit
Efficiency Gains can come in many forms: higher utilization due to virtualization and tools that lower labor costs. Some costs will change from capital investment (CapEx) to a pay-as-you go (OpEx) model. Services expensive to maintain or upgrade should get high priority.	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems	• Improved asset utilization (server utilization >60-70% • Aggregated demand and accelerated system consolidation (Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user
Agility Rapid automated provisioning of computing and storage resources putting IT agility in the hands of users. Priority should go to existing services needing long lead times to upgrade or increase / decrease capacity and new or urgently needed services to compress delivery timelines as much as possible.	• Years required to build data centers for new services • Months required to increase capability of existing services	• Purchase as a service from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs
Innovation Compare current services to contemporary marketplace offerings, or look at their customer satisfaction, usage trends, and functionality. Priority should go to services most benefiting from innovation.	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-averse culture	• Shift focus from asset ownership to service management • Tap into private sector innovationo Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)

Decision Framework For Cloud Migration

The framework is flexible and can be adjusted to individual agency needs.

Select

- Identify which IT services to move and when
  - Identify sources of value for cloud migrations: efficiency, agility, innovation
  - Determine cloud readiness: security, market availability, government readiness, and technology lifecycle

Provision

- Aggregate demand at Department level where possible
- Ensure interoperability and integration with IT portfolio
- Contract effectively to ensure agency needs are met
- Realize value by repurposing or decommissioning legacy assets and redeploying freed resources

Manage

- Shift IT mindset from assets to services
- Build new skill sets as required
- Actively monitor SLAs to ensure compliance and continuous improvement
- Re - evaluate vendor and service models periodically to maximize benefits and minimize risks

Catalyzing Cloud Adoption: Shift from Asset Ownership To Service Provisioning!

For cloud computing to flourish, the following must happen according to the Federal Cloud Strategy.

Security

- Centralize certification and accreditation for cloud solutions
- Prioritize security controls to counter the most serious threats
- Use near real time security dashboards to facilitate continuous monitoring
- Integrate identity management

Standards

- Define and evolve standards to ensure interoperability, portability and security
- Propose and test interim standards
- Publish cloud computing business and technical use cases, a neutral reference architecture and taxonomy

Procurement

- Develop vehicles to accelerate the purchase of cloud solutions
- Maximize strategic sourcing to buy cloud solutions
- Eliminate redundant and inefficient vendor certifications
- Integrate needs of state and local governments

Governance

- Set policy and enforce budget priorities
- Align with regulatory and legal frameworks
- Drive government-wide adoption
- Collaborate with international entities

Source: Federal Cloud Migration Strategy, Vivek Kundra, Federal CIO, February 2011

Videos

Future Visions (from the Federal Executive Forum)

Mike Krieger
US Army

Jack Wilmer
DISA

Dawn Leaf
NIST

Reach Your Cloud Potential

Cloud experts offer practical advice on how government can turn potential cloud benefits into real ones.

"What do I do first? How do I get there? Who can help me? Is there guidance?"

Those questions are top of mind for IT executives and staff charged with meeting their agency cloud computing goals.

For them, the challenge moving to the cloud is not the technology. There are numerous deployment models – private, community, public, or a hybrid combination.

The challenge is changing from an ownership culture to services-on-demand culture.

However, government cannot outsource responsibility. So, more than ever, government managers will need to rely on the practical experience of private sector cloud providers to reach their technology transformation goals. Providers such as:

- **Steve Wallo**
  Principal Systems Architect, Federal
  Brocade
- **David Blankenhorn**
  Chief Cloud Technologist
  DLT Solutions
- **Jeff Bergeron**
  Chief Technology Officer (CTO), U.S. Public Sector
  HP
- **Steven Peacock**
  VP Federal Infrastructure and Cloud Services
  Unisys

All have government customers who are faced with the cloud migration process. They shared their views on how to reach your cloud potential with OTFL editor Jeff Erlichman in the OTFL Roundtable.

DLT's David Blankenhorn: Not if, how?

"Enough with the IF already. Let's talk about the HOW?" exclaimed DLT Chief Cloud Technologist David Blankenhorn.

"The market dynamics coupled with technological innovation have reached the point where cloud technology is changing the way we manage and consume IT services," said Blankenhorn.

"We've seen this before with the shift from mainframes to client-server computing. We've seen it with the Internet proving that it is a viable platform for business-to-business communication and business transactions. Now we are seeing it as a new way to deliver IT service with greater efficiency and scale at significantly lower costs."

Email, collaboration and test/development are the three "low hanging fruit" areas most agencies will move to the cloud to meet their 2012 deadlines. And pressure will continue to look to move more applications to the cloud.

"Beyond Email and Collaboration, CRM is a clear winner at the moment," said Blankenhorn. "We also see agencies leveraging IaaS for the deployment of web services."

Overcoming Barriers

When it comes to cloud adoption, policy is probably the most significant barrier according to Blankenhorn. "Eventually, we'll be able to purchase IaaS through www.apps.gov, but in the meantime, agencies are left on their own to work through the labyrinth that is policy, governance, security, and contracts."

On the security front, Blankenhorn acknowledges there is a challenge, "Not because cloud providers lack security, rather it is because we have a failure to communicate between government and the providers."

Policy and security requirements haven't kept up with cloud technologies, and on the flip side cloud vendors who have typically been incubated in the private sector don't understand the government asserted Blankenhorn.

"These cloud providers want to provide their services to the government, and as soon as government can provide clear requirements based on cloud technologies as opposed to legacy owned our outsourced data centers we'll see the cloud providers innovate and adapt."

Culture issues can be overcome through exposure and education said Blankenhorn.

"Cloud providers and companies like DLT Solutions need to work more closely with government IT folks to help them better understand how to leverage both public and private cloud technologies. Government IT also needs to give IT professionals the opportunity to look at and evaluate cloud technologies."

Keep Relevant Skills

The cloud is a fundamental shift in the approach to technology. All professionals need to keep their skills relevant. The same is true for IT said Blankenship.

"This means moving skillsets further up the stack. If you do racking and stacking and operating system installs, it's time to look at automation and provisioning. If you are doing resource capacity planning, move up to service capacity planning," he urged.

Most importantly, "stop thinking components and start thinking services. And everyone should learn to understand Service Level Agreements (SLA), as this skill is becoming increasingly important in all aspects of our lives.

Being able to read an SLA will enable you to understand the services being offered by cloud providers to government, but it will also help understand how those pictures you posted on a social media site can be used by the provider."

HP's Jeff Bergeron: Now, It Comes To Execution

"The market has a definite understanding of the benefits of cloud; we have gotten through the education process of educating on what cloud is about," said **Jeff Bergeron**, Chief Technology Officer (CTO), U.S. Public Sector at HP.

"Now it comes down to execution."

With more urgency Bergeron said his clients are asking: It is mandated through the 25 point plan, so where do I start? What makes the most sense?

"We see a sense of urgency with the 25 point plan. It is important for agencies to understand what can feasibly be moved in the timeframe outlined; ones that can easily transform into a cloud environment," explained Bergeron.

Discovery Workshops

HP's cloud strategy is centered around four distinct pillars. They are: transform, build, consume and manage/secure. Within each one of these pillars, HP is delivering capabilities.

HP provides government cloud consulting services to help clients define the transformational roadmap to get to the adoption of cloud services.

"As in any IT transformation, go back to the 1990s and client server, there is always this evolution of where do I begin?" noted Bergeron. "I can't rip out everything I have today; but how do I get on the journey of where I want to be?"

A very individualized agency plan needs to be put into place in order to transform into the cloud Bergeron explained. "The challenges faced may or may not be faced in other agencies."

To help agencies cope with the challenge HP sponsors Discovery Workshops to help agencies define their cloud roadmap.

"Discovery Workshops are just that," Bergeron explained, saying this is an initial setting where we can sit down with agency CIOs, IT professionals and business owners and talk about the impacts of the cloud.

"We can layout in a methodical way the different areas that will be impacted," said Bergeron. "From security to Human Capital management to IT infrastructure to apps, we break it down into its simplest form in order to be able to define the transformational journey for clients."

"We even get into business management and financials and potential impacts. We present a holistic picture with the incremental steps that need to take place to transform."

Human Capital Impacts

"The other aspect we like to talk about through our transformational journey conversation is the human capital impact and the change management that needs to occur during this transformation," Bergeron said.

From a role based perspective, "if I put myself as an agency person or contractor, who would be the ultimate consumer of services, how I go about getting resources will change in the future," said Bergeron. "I will be able to access them on-demand when I need that, so how does that change the day?

Further, what is role of CIO under a cloud construct? Are they more of a service provider? And what services do I need to enable mission outcomes and consumers need to perform their jobs? With cloud there will be an evolution of roles and responsibilities.

"These are new concepts and ideas that enable IT, so the workforce needs to be prepared for this and trained. "

Security In A Hybrid Environment

Cloud services will be delivered in a hybrid environment, a cross between public consumable cloud services along with in house private cloud services said Bergeron.

HP is embedding its cyber capabilities into its cloud offerings providing the ability to do continuous monitoring, a must according to FedRAMP.

Email, collaboration and Development/Testing will be the norm in the next 3-5 years said Bergeron. Looking out to the future he envisions HR and financial management applications, more of the "back office" apps.

"It is the agency management tools around human capital and financial management that are the next evolutionary steps."

Brocade's Steve Wallo: The Simple, Easy-To-Use Cloud

At Brocade, Stephen Wallo is Principal Systems Architect. He says their vision is first and foremost to make things easy and simple to use.

"The cloud is more than just a pool if IT assets, it must be viewed as a service," said Wallo. "Every component needs to be cloud aware; and they must be agile, optimized, efficient and secure. There is a lot involved and a whole different approach as to how things were built in the past."

Wallo said agencies are seeing how virtualized servers are working in the cloud — and they like what they see.

Now, they are beginning to look at their network infrastructure in relation to the cloud asking "what do I need on my network so I can make sure things are agile? Can I move things around efficiently? Can I utilize what I have? Is it cloud aware? What is the security?"

He noted the biggest thing he is seeing within agencies is there is no longer just a network team or a server team or a storage team; now IT is treated more as a service managing a pool of resources.

To do that people must collaborate and get rid of fiefdoms. "A lot of people have knowledge in all of the areas, not just specialized in one area so the skill sets go beyond understanding more than just one little component," said Wallo.

Moving to the cloud is bigger than just saying "I want to do it". Most importantly Wallo said everything must work with what the agency already has, leveraging resources to keep the network running at all times.

Different Approach

As a networking vendor, "we take a different approach, asking: what does it mean to be in the Cloud; how does that apply to virtualization; how can we make it simple and easy to manage?

So it has to be agile, has to be able to move things around, self-heal, simple and manageable," said Wallo.

Wallo explained how Brocade uses Ethernet Fabrics. Compared to classic hierarchical Ethernet architectures, Ethernet fabrics provide higher levels of performance, utilization, availability, and simplicity.

"We have to get to point where the network is virtual, agile and optimized. We are taking advantage of what the server virtualization started and storage followed. It all has to morph together as a service rather than just a bunch of individual resources tied together."

Wallo advises program managers when they talk to their IT departments about the cloud, they ask these pros to seek out as many companies as they can.

"Ask what their vision is; ask how do I grow into something that enables me to do virtualization and cloud?" counsels Wallo. "You can't get there immediately; you have to ask 'how do I get to where I want to go?'"

Over the next few years Wallo thinks cloud standards, acquisition and security will be in place. "Then you will see technologies arise that leverage what's already available and providers will be able to leverage each other's core strengths to build new capabilities."

And of course, it will be simple and easy to use.

Unisys' Steven Peacock: Use a Hybrid Enterprise Strategy

Steven Peacock is the VP Federal Infrastructure and Cloud Services at Unisys.

Over the past 18 months Peacock has met with numerous Federal CIOs. During that time, he has seen a change in their attitudes from resistance to cloud (with security being the stated obstacle) to embracing the cloud especially after the mandates of OMB's 25 Point Plan and Federal Cloud Strategy.

Still there are common themes and concerns from CIOs to moving to the cloud said Peacock.

First is security, which Peacock said was used as the "buzz kill" for cloud. "But with the release of the OMB directives and Cloud Strategy, people stopped stonewalling," said Peacock. "Now they know they have to solve the security issue."

Second is the cloud's unfunded mandate with no new staff dedicated to move apps to the cloud. 70 percent of spending is on existing infrastructures said Peacock. "If you want to move to cloud it requires funding and staff to get this done."

Third is the recent failure of the Amazon cloud, which illustrates the lack of control issue. Agencies need to know that they have the full control over these apps, after they move them to someone else's infrastructure. That puts pressure on IT pros to have the right skills to manage cloud environments.

"We see skill changes when working with clients," said Peacock. "We see a lot of people combine their skills and skilling up for these new technologies. Like when doing virtualization, there are a lot of new things to learn. The IT staffs are excited because it is their future."

IT pros are going to need these skills because Peacock says the last pressure is from their users to move apps to the cloud. "When you see Microsoft and Cisco advertising the cloud on TV, pressure mounts from users to move quickly; it has almost set up a competitive environment between CIOs and this is good."

What To Do Now?

With cloud deadlines approaching, Peacock explained that just recently Unisys announced a new approach to help agencies and CIOs deal with issues related to moving to the cloud.

"Issues can be systemically and effectively addressed by taking a different approach to cloud," Peacock said. Based on the practical lessons learned from experience, Unisys calls this their Hybrid Enterprise Strategy.

The Unisys Hybrid Enterprise strategy is the foundation from which Unisys guides CIOs to a future-state data center environment that is borderless, virtual, automated, visible and secure, while reducing risk and increasing efficiency said Peacock.

Peacock explained that "Hybrid Enterprise" is a composition of cloud, non-cloud, internal and external IT service delivery models that remain unique entities. These unique entities are bound together by "an integrated management environment, and common technology, processes and policies to optimize agility, enable data and application portability, and reduce risk."

By using a hybrid enterprise strategy that integrates with existing IT management technologies, users avoid the "Cloud in the Corner" approach said Peacock.

"If you keep adding delivery models you will lose controls and place security risks at a higher level; and risk duplicating resources and raise your operations costs. Now is the time to start thinking weaving them all together before the multiply and grow," counseled Peacock.

By taking the strategy and specific methodology we think they will get there faster and safer noted Peacock. "This enables CIOs to maintain control, manage governance and compliance, reduce IT costs, and tackle organizational issues, all within the context of a virtual, federated data center footprint."

Future Proofing Your Infrastructure

Look inside the Hybrid Enterprise Strategy and you'll find a series of frameworks and methodologies for adopting these cloud technologies and business models that always focuses in three areas: apps, infrastructure design and management.

"If you evaluate using those three areas, you can look at new technologies and capabilities and be assured that you are future proofing your infrastructure," said Peacock.

"So if a new provider comes up with a cloud capability of some sort, you want to be able to look at it across the three different areas and make the checklist: Is it secure? Does it affect my storage? Is it backed up securely? Do I have the process and policies to address that capability? Does it require different access and tech constraints? This is a structure or framework around which you can adopt new tech and business services and you have covered all your bases."

And not only can you use the strategy to meet upcoming deadlines, it will actually speed the process Peacock asserted.■