

Government agencies are under a mandate to look to the cloud to deliver services for their users, and many have already shifted such things as email and collaboration tools to the cloud. But, now the early hype is over, questions of security, cost and suitability overhang future agency decisions.



Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems



Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation



Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

Q1 Is the concept of the cloud now pretty much set, or is there more to come? Will the cloud five years from now be the same as the cloud of today?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

I think it's set as far as the basics of the cloud are concerned, but how you use and deploy the cloud is going to change over the next five years. There's a similarity with where the Internet and web services were 10-15 years ago. The basic technology hasn't changed much, but the way people apply the technology has. I anticipate similar development with the introduction of new applications in the cloud.

There are different ways to structure and use the cloud today. In particular, within agencies you'll see a wide variety because of the diversity of agency missions and their specific requirements, including security.

A cloud architecture built using open standards allows for quick and rapid integration of new technologies, allowing agencies to keep pace with advancements in technology over the next five years. The cloud is an ever-evolving resource. The scalability, flexibility and reliability of a dynamic cloud will deliver capability based on mission needs.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

The concept of the cloud as a business strategy is pretty well-defined, but the future will certainly see much greater adoption of the cloud and many new and innovative ways to leverage technologies and offerings. As a consequence of that, cloud offerings will continue to mature to reflect the kinds of investments that will be made in this domain. And while current adoption is mainly driven by IT, we see future adoption driven more by the mission.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

We're in the earliest stages of what will be a long and rewarding journey. We've already seen the early promise of the cloud delivered through different public and private cloud offerings and, as it continues to mature, I think the cloud will transform IT from a back office function to one that is tightly aligned with the business side of organizations. The payoff will come from how you broker and orchestrate the delivery of services between public and private clouds.

Ultimately, the cloud will end up being just another part of the background that the IT organization will use to connect with its user base again, by brokering business services that will greatly improve service delivery and mission execution.

Q2 How effective are government mandates such as “Cloud First” in promoting the use of cloud services in government? What else is needed?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Saying you want to do something is one thing, but then you have to go out and actually contract for and build pilots to kick things into gear. I’m seeing this happen as agencies become more comfortable with the cloud concept.

We’re getting past the mandate phase and starting to see in a number of different solicitations that agencies want providers to demonstrate how they are going to deploy their solutions in a cloud environment. This allows us to move beyond concepts and into real world applications, helping agencies become more comfortable with the cloud and what it can do for them.

As with any organization, there is a mix of those who want to keep doing things the way they’ve always been done, and others who want to change. To see cloud services adopted, agency leaders need to advocate for cloud and flow that message into their organizations, helping to unify the two worlds and maintain focus on the mission.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

“Cloud First” has been an effective catalyst to get government agencies thinking about what should and should not be in the cloud and to take efficiency and agility into consideration as they move forward with new applications. In practice, we help customers understand the transformational nature of cloud services on the people, processes, and governance of an organization’s business.

We are definitely past the early hype stage, and now agencies are thinking more about how to better adapt the cloud to their missions. Further initiatives such as Shared First and now FedRAMP have further enabled adoption. Future adoption will increase as acquisition policies and standards are tuned to cloud services.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

Well, they certainly get peoples’ attention. The Cloud First mandate is a well thought out and pragmatic approach, and managed to take into account both the government CIOs’ view of their agencies’ missions and also an understanding of what is happening in the industry right now. Then it established a set of drivers to move the government forward in delivering services to citizens.

If you think back to where we started with this, service oriented architecture was a hot topic a few years ago, then the heat ramped up around cloud. Now we’re talking more and more about mobility and Big Data. When taken together, these technologies moved the ball to get us to a higher state of productivity and to a higher level of performance, all at a lower cost. When these mandates are well considered, with input from both government and industry, they do tend to push things forward at a quicker rate.

Q3 What does the shared IT services strategy recently released by Federal CIO Steven VanRoekel mean for the future development of government cloud computing?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

There is tremendous value in creating shared services across different agencies, including reduced costs. There should definitely be reuse of these services. There is no question that sharing services will be a core strategy.

The challenge is how to manage and coordinate the varying requirements, critical applications, diverse users, missions and modernization acquisitions of multiple agencies. Who leads and who follows? Agencies should collaborate to focus on what is common. If one agency can leverage what another agency has created, they are starting at an 80 percent solution rather than starting from scratch, and delivering solutions faster while saving money.

Integrated working groups will help agencies identify and prioritize needs, coordinate efforts and provide a forum to establish common requirements up front, thereby helping to drive cloud adoption.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

A primary reason agencies now want to use the cloud is to be able to address common mission needs while reducing costs. In that sense, they've already been applying this shared services mentality to realize savings across their core lines of business. Will the government's shared IT services strategy lead to a broader consideration of the cloud for these types of services? I believe it will. The strategy will drive a wider use of the cloud for services, but it will depend on the particular situation of mission-added value and the experience each agency has had with the cloud.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

Both he and Richard Spires, the Department of Homeland Security CIO who co-chairs the CIO Council, put a great deal of energy and forethought into it. I think we'll see a lot of value generated because of it.

A cloud-based infrastructure that frees up the back office, that's put together with a more business-focused service delivery, creates a very synergistic arrangement. Add data center consolidation, which by itself may not be the greatest thing, but when put into the mix it's all extraordinarily important. IT shared services builds on that, allowing agencies to eliminate fragmentation of services and create centers of excellence that focus more fully on the mission without putting a lot of energy into back office operations.

Q4 Security of the cloud is still the biggest concern for government users, but is this warranted? Some say the need for security will soon drive cloud adoption rather than hinder it, do you agree?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Security will drive cloud adoption. The cloud takes data that is accessible now through many Internet access points, virtually and physically, and collapses it into one data center. This provides a controlled interface to the rest of the world that limits and manages access.

In this sense, cloud technology is actually more secure as there are fewer points of entry and locations. In addition, with cloud technology you never really know what computer or server any particular piece of information is on, making it difficult for bad actors to find it.

Again, the cloud is following the same adoption path as the Internet. According to Pew Research, while 82 percent of American adults use the Internet only 61 percent use online banking, an increase of just 8 percent over the past five years. I believe that the cloud is a secure technology, but developing trust in that is going to take some time.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

Security should always be a concern when sensitive data is involved. If you look at any conventional cloud model, the private cloud is seen as more secure but also more costly than the public cloud, so the mission will determine what cloud to use. The security models and multi-tenant issues that drive the debate now continue to evolve at a rapid pace, and I think agencies are adapting more to the realities of cloud security and are more aware of what they are, or are not, prepared to put into the cloud. In some cases, the visibility into an organization's IT assets that a public cloud provides and the basic layers of network defense offered by public cloud providers may be an improvement from what the organization has today.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

Security is a persistent and very real threat, but you can't let that lead the business. You need to bake it in upfront so that the cloud isn't inherently less secure than a given organization's overall infrastructure. You have to have a clear vision and strategy for where you are going with cloud, include security as an operational component as you begin to implement it, and continually monitor what's happening with all of your applications.

The good thing is that you really don't have to secure everything to the same degree. You need to find those valuable pieces of information that may need to be better protected than most and focus your energy there. I would say that 70-80 percent of the information that government deals with isn't at this level. You don't want to build a set of security requirements that are costly and difficult to operate and maintain to protect information that isn't as confidential or needs to be as well protected. Just focus on the crown jewels.

Q5 What can agencies do to prepare for the Federal Risk and Authorization Management Program (FedRAMP), in order to make its application as easy as possible for their cloud implementations?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Agencies need to work closely with FedRAMP and make sure they understand what the standards are, what their agency's prioritized needs are, what criteria are being used to evaluate vendors, and how third-party assessments are conducted. They need to be proactive in talking about where they are going with their cloud implementations and what it is they want FedRAMP to do for them. FedRAMP has designed a number of tools to help agencies, including a security assessment.

Ultimately, understanding agency needs and the supporting priorities is going to be key for successful cloud implementation.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

FedRAMP is a very comprehensive approach so we do not foresee the need for agency-specific requirements. However, since FedRAMP is allowing agencies to include additional agency-specific requirements on top of the FedRAMP baseline and recommendation, there may be a temptation for agencies to revert to their previous requirements due to familiarity. Agencies would benefit from taking a holistic view. By understanding and scoping their own environments and thinking about what should truly be unique to the environment, agencies can be better prepared. FedRAMP will be the foundational component and will ultimately simplify certification and accreditation.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

FedRAMP is just a great idea. It gets us out of this duplicative workflow and process that every agency experiences in order to find a cloud software package and infrastructure provider and put those things together. As agencies purchase goods and services, they have to certify and accredit those as good enough for their purposes. On average it would take around \$200,000 for each of those certifications only to have them end up as a piece of paper sitting on a shelf somewhere because the system would change over time.

FedRAMP now allows us, through the GSA, to certify an application just once and all agencies can be assured it meets their requirements. It's a huge cost savings for the government. Agencies need to ensure they understand all of the controls included in FedRAMP, and where GSA is in the process of standing up the program.

Q6 What are the next candidates for agency applications moving to the cloud now that "low hanging fruit" such as email and collaboration tools have been identified for the first wave? How do agencies make those selections?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Agencies are looking to the cloud to save money as they have invested a lot in their legacy systems. Now they want to leverage their investment, drive cost out and improve capability through modernization via the cloud. They will look to systems and applications they can upgrade rapidly through the cloud, allowing them to quickly retire legacy systems to get the biggest bang for the buck.

Agencies should focus first on projects that have less stringent security requirements since they likely won't involve highly classified information. There will be some smaller applications that won't be touched, as they won't provide a significant return on investment.

Agencies should then go to the next level where they can use the cloud to share data services and combine data into common data repositories. It will be a crawl, walk, run approach.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

The first migrations have focused for the most part on low risk, back-office functions. Consistent with Shared First, it is likely there would then be migrations with a series of mid-tier applications that are more complex with

higher value and closer ties to the mission.

To make those migration selections, there definitely needs to be a structured approach. Factors like mission, technology, security requirements and ROI all have to be considered. And it's important that they don't look at the cloud strictly from a technology standpoint. Before any consideration of technologies, the core impact on mission and mission agility as a result of the migration to the cloud needs to be incorporated throughout any applied assessment. The challenge is determining an approach to ensure this balance. Northrop Grumman's methodology, MApps2Cloud, encompasses all these considerations through a web-based tool. This MApps2Cloud solution provides a path for building and executing roadmaps to ensure a suitable, cost-effective, secure, step-by-step approach for migrating our customers' critical mission applications to the cloud.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

It's extraordinarily important that they have a clear idea of where they want to go, because they need those turn-by-turn directions for the cloud. First, they should be looking at their portfolio of applications through a diagnostic lens to know which is right to put into a cloud, be it a private or public cloud. Then they should take that lens and focus it on where there is a lot of custom workflow to determine if there are redundant applications and see if a cloud-based service could do the same job. That's where the biggest bang for the buck is going to come from. The larger scale transactional systems in HR and finance will likely be the next step in the maturity of this movement to a cloud-based infrastructure.

Q7 **Moving applications to the cloud is expected to save agencies money, but it's not cost free. What do agencies need to do to assure a least-cost transition?**

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Agencies should first invest in an ROI assessment. For example, it may be that all they need to do to save money in the near term is to move an app onto common hardware. Reducing hardware and transitioning to commodity hardware can be an immediate costs savings.

I do think agencies need to take a long-term view when it comes to the cloud, but they don't need to take huge steps to get there. They can quickly get an instance of the cloud up and running, have it work in parallel with legacy systems, and gradually migrate to the cloud. You can actually do the migration better by building a little at a time and evolving to deal with changing needs and requirements. I think that's far better and smarter than developing and adhering to a detailed multi-year development plan.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

We utilize a multi-stage maturity model to gauge an agency's progress on the path to cloud computing. If an agency has already taken steps to accomplish this foundational work, then the cost to transition to the cloud will be much reduced. Again, it's a journey and not a specific solution. There's the discovery phase followed by a standardization phase followed by a consolidation phase.

For example, agencies may have done some consolidation in the data center to save on hardware resources, but how far they can go beyond that to transition to the cloud will be a function of cost and adaptability. An agency may find that some applications are not able to leverage the cloud. If they were to do things over, they could use our maturity model to discover what is in their environment, standardize applications, then consolidate and look for cloud offerings that work best and eliminate redundancies to save money.

Also, if they assess the application security posture, there could be some intangible savings in moving towards a more standard model that better protects applications and avoids more costly "siloed" approaches to compliance. If agencies don't follow this phased approach, they can find themselves adopting something that will break a process that was working just fine before.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

Around 80 percent of the money spent in IT now is for operations and maintenance. A straightforward enterprise data center consolidation is going to save around 10-15 percent of current costs. But by implementing a cloud-based set of technologies you could see a 66 percent reduction in operating expenses, in addition to capital expense savings. And you don't need large amounts of money to do this.

There is a ton of ROI to be had in this area. Agencies just need to be thoughtful about where they are trying to go and in what areas they are trying to improve business. Then, using the cloud, they can quickly serve up new products to their users. They get very innovative capabilities quickly, and at low cost.

Q8 Standardization has been considered a key development by government cloud users. What's the progress been in developing those standards?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

A number of agency CIO offices are working together to come to an agreement on what cloud standards are and how they can be implemented in government. This is important because it makes sure everyone is on the same page and, once they do agree on standards, it makes it much easier for everyone to build to them.

Agencies are starting to use those standards in various cloud pilot programs, and the results of these programs will provide a better idea of how to drive and shape the standards because everyone will have had a chance to try, use and test them. But they do need to stay in tune with the commercial world so they know how cloud standards are evolving to avoid reinventing the wheel.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

There are a number of groups that are involved in trying to define the cloud and cloud offerings. We've looked to the National Institute of Standards and Technology (NIST) as a kind of normalizer for these standards and common definitions, but those efforts haven't yet made it past the point of establishing common definitions. While many existing standards are applicable to cloud computing, new standards, especially for tough areas like cloud interoperability and workload portability, are yet to come. Standardization is certainly an important component of long-term cloud adoption.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

It's a very nascent area, right now, though there are some industry organizations beginning to address standards for the global cloud space. You have some standards for data portability, for example, to make sure data can be moved from place to place in the cloud.

In terms of what happens internally when organizations go to the cloud, however, that's different. To employ an internal private cloud infrastructure you need to standardize everything, from the bottom up, and you need to tie things down from a security standpoint. You standardize the development languages so you can reuse components and develop services just once for the entire organization.

People need to go into this IT transformation with their eyes wide open. They need to have a thoughtful strategy, and a set of frameworks and business drivers that gives a direction for decision making. You absolutely must be aware of the decisions you are making and what that means for things like data portability, because the cloud products and services in five years are going to be very different from those available today.

Q9 What are some of the most important best practices that agencies can use for moving services and applications to the cloud?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

The three most important are:

- Implement pilot studies to help evaluate what should move to the cloud and when
- Use of an agile and modular development process, to build a little and test a little
- Leverage open source technologies and commercial standards

Agencies will also need to understand what cross agency services they want to adopt, and how they plan to manage and govern the cloud. For example, if one agency wants to use an existing service 24/7, but the originating agency only operates it 8/5, how do we leverage the investment without altering the mission of the originating agency?

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

Understanding the agency's level of cloud readiness and maturity is key. Agencies first need a trusted advisor that can help determine their requirements with regard to their mission and applications. The cloud will help from a process solutions perspective and will help save on labor costs. But to maximize those benefits, agencies need to understand the implications of these decisions.

An assessment toolkit will help prioritize the best cloud solutions based on the agency's business strategy. If an agency is looking to reduce the level of labor and technicians they have in the field, there are some cloud solutions that will offer better availability of equipment. Virtualizing the server environment, by definition, will cut demand for technicians, but agencies may not be comfortable with a higher percentage of virtualization than physical servers. Again, this will be based on the business strategy of the agency.

For example, a typical cloud application can be storage. If an agency doesn't discover what types of storage they have in the enterprise and standardize across that, then they may find that such things as their data replication for disaster recovery is affected when they are buying cloud storage. Without standardizing across the environment, buying something that helps one part of the agency can end up hurting another part of it.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

It has to be done on the back of a business-driven, mission-driven agenda. But remember that this is not a silver bullet for everything that ails an agency, so due diligence is imperative. The practices around IT service management and business management and the need for the right set of business intelligence tools must be baked in to an agency's approach. If you do all of that you will see a much more agile service delivery network focused on solving those issues of importance to the business.

Q10 Can the cloud be used by agencies as a strategic asset? How can they "shape" the cloud to meet specific needs?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Absolutely. Moving to the cloud will help agencies save money and improve mission capability and performance. Co-locating apps and data in a central data center will allow agencies to easily combine the data with new applications, new services and missions. Now the cloud is a strategic asset as it houses the enterprise.

Developing new, mission-specific capabilities can be done quickly in 30-60 days in the cloud, allowing for rapid delivery to users. But the beauty of the cloud doesn't stop here.

Users are now part of a feedback process where they can see and react to the new services designed to improve how they carry out their mission. This is certainly another example of the cloud being a strategic asset. Getting direct user input and reaction that helps agencies fine-tune capabilities for successful execution and management of their missions.

Another advantage is agencies leveraging each other's services. Some agencies are participating in integrated working groups, putting teams together with members of varying roles and responsibilities, and tasking them with solving various problems by using the cloud and shared services.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

It's important to keep in mind that the cloud will enable a greater level of agility and flexibility for agencies to allow the cloud to become a strategic IT asset. Hybrid community clouds - a mix of public and private clouds - can perform this function. Simply trying to shape a public cloud to provide this level of agility is difficult because the scale of that environment, which has to accommodate many different users, will drive the results and not the demands of any particular user.

Again, it depends on the mission of an agency. In order to have maximum agility, for instance, a private cloud may be required.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

One of the issues folks have had with IT organizations over time is their inability to move quickly, to see a problem within the business and solve it rapidly. The cloud does away with that. Today, with cloud technologies available,

we can promise a faster, better, cheaper and more secure way of delivering services. And we can say it's an asset that allows for a constant discussion about the mission, and how to quickly put together products and services that the business side of agencies can use to improve things. They feel in control again, enabling them to be very entrepreneurial and to generate more ideas that quickly produce tangible assets for making those improvements.

Q11 Who should be involved in contracting for cloud services? Is this still the responsibility of the agency IT department, or should others take the lead?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

We expect cloud to go beyond email and ISP to be used on projects to field common infrastructure services and customize mission capability, where it's more about migrating applications to the cloud. Based on this, contracting cloud service needs to move from the IT department to a core team of agency mission stakeholders who have the necessary domain knowledge and mission expertise and can include acquisition, engineering and general counsel. This unified approach will help address mission-specific capabilities holistically.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

Mission-focused organizations will be able to take the lead in evaluating the various technology solutions that are needed because they are the ones that provided these capabilities in the past, whether it was called cloud or something else. But government contracting organizations such as the General Services Administration, and governance organizations involving an agency Chief Information Officer (CIO), also need to be involved because the governance aspect is very important.

Governance cannot be ignored because it's critical to ensuring that cloud solutions are in harmony with organizational policy. You may have really strong organizations that can lead in terms of developing specific software capability, but if what they do is not aligned with the CIO's objectives and policies then agencies will have a challenge implementing anything.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

The IT organization should be in charge of these acquisitions. It's all about making IT highly agile and highly responsive to the business of the agency and about delivering the best value on behalf of the organization.

That said, the acquisition staff should be at the table from the very beginning, from the initial meeting and discussion. The best acquisitions are those done with all of the stakeholders involved. The IT folks lead it, but the business and acquisition groups should also be there along with the chief financial officer to make sure very clear goals are set on what the business is trying to achieve with the cloud, and that everyone is lined up in support behind it.

Q12 Are there any services or applications that agencies should not move to the cloud, and if so why? Are there situations where applications would normally be candidates for the cloud, but nevertheless shouldn't be moved?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

I see two scenarios where moving to the cloud might not make sense. First, there are some legacy systems that are attached to small missions and moving them to the cloud isn't going to benefit the mission or deliver any reasonable ROI.

Second, some services are not using Internet technologies because the data or missions are just too sensitive. Because of the stringent security requirements they are unlikely to move to the cloud anytime soon.

When agencies focus on their missions and let that drive their cloud implementation strategy, rather than view clouds as a cure-all, we'll see clouds being utilized for the right purpose, becoming a true strategic asset.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

There are certain applications that shouldn't be moved, mostly legacy applications that have very specific and unique functionality that the cloud can't efficiently support. But each application needs to be evaluated as to whether it makes sense to move it to a cloud or not. Just because it's a legacy application you can't assume that it's not a candidate for moving to the cloud.

While there is merit in all applications moving towards the cloud, it would be a question as to what degree. Relocation of an application to a more concentrated computing environment, but leaving the application "as is" would save operational costs. Standardizing elements of the application would allow sharing and reuse with other applications, also resulting in savings. Finally, any decisions about running the application in a shared, virtualized, multi-tenant data center or cloud will most likely be driven by the application architecture, the security of the data the application represents, and the operations concerns such as multi-level security and information spillage.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

This goes back to the question of whether the cloud will still be the cloud in a few years, or whether it will be just a part of the way business is regularly done. I think that's exactly what's going to happen. Right now, when you look across the portfolio of applications, you have to be thoughtful about what to move to the cloud, and you have to have a framework for making that decision. Ultimately, things are going to fall out pretty readily into this new dynamic we call the cloud.

I wouldn't suggest agencies start off with their most complex transaction system that has maybe 50 legacy interfaces. Taking the most complicated parts of the portfolio and moving those over would be a recipe for failure, because there's a lot of fragmentation to address internally within the existing environments. It doesn't mean you can't eventually put those into a private cloud infrastructure as you build that out, but it's a much longer-term proposition.

Instead, federal agencies need to identify systems and data with the least security issues, without a great deal of legacy complexity and, for the first movers, without privately identifiable information. That's why organizations have started by moving things such as email and collaboration to the cloud first. The next thing we'll see moving to the cloud is customer relationship management, which already has an eight-year history in the private sector so it's a very mature process.

Q13 How do agencies decide which flavor of cloud – public, private, hybrid, community – is best for them?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

It depends on the agency missions and needs, and I expect you'll see an application of all of these kinds of clouds at some point. Security requirements and costs will influence cloud selection and whether or not an agency wants to own their cloud or contract with a provider. For example, an agency doesn't necessarily need to own a cloud if they are only running email or other non-mission critical applications.

Agency needs will change over time, and five years from now I expect those needs to be different. An agency that uses a hybrid cloud today because it wants to get the cost benefits of the cloud but is still sensitive about sharing its data will get more comfortable with how the data is being protected over time. Then we'll see the adoption of architectures such as a community shared cloud, where it shares services and its data is also in the mix.

A major benefit is that it's fairly easy to mix the various flavors of the cloud and to change those flavors over time depending on how agencies want to use the cloud. It just means changing how software is loaded and how applications are deployed in the system. So it can be an IT function to change from a public cloud to a private cloud hybrid.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

This is a real challenge. There's a balancing act needed to determine what's really the most cost effective solution from a narrow mission and business perspective, as well as what is compliant with the agency's unique requirements. While a public cloud solution typically offers the best cost advantage, the risk with a public cloud may be too high for many federal applications that involve sensitive or personally identifiable information.

On the other hand, agency-specific private clouds can restrict government customers from being able to tap the full potential of cloud computing. The Federal Government won't have a "one-size-fits-all" approach, since different flavors of cloud carry different levels of cost and risk. The final decision will be based on what agency applications are involved and what the business need is dictating.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

There are a number of things that have to be weighed. The value of the data you are dealing with, for example, and whether it's information that is open to the public, if it's law enforcement information, or whether it is regulated under the privacy act. Are there critical infrastructure protection issues that have to be considered? And what's the value to the business of moving things to the cloud? This and more will have to be weighed to see what type of cloud is the best candidate for agency needs.

Agencies will also have to decide what mix of cloud types can satisfy their requirements. As data consolidation programs progress we'll see agencies building out their own internal clouds, but you have to have sufficient scale. If at least some of the information is public facing, agencies have to ask themselves if they want that going into a private cloud, where they'll likely have costs that are somewhat higher than in a public cloud.

Right out of the chute they'll need a solid strategy, because they'll have maybe one private offering and two or three public offerings. It's very important that the business drivers are out front for security and all of the other requirements that go into the weighted decision criteria that tell you where you need to store them. It has to be very well laid out and very well executed, and it has to be controlled going forward by using continuous monitoring to make sure everything is operating in a high performing and continually improving state. So it's not simple.

Q14 Is there such a thing as a cloud ROI? How do agencies measure the effectiveness of the use of the cloud compared to initial expectations?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

Agencies are now looking at how to measure cloud ROI and include the traditional costs they can track, such as application license costs, hardware maintenance costs and operation sustainment costs at different sites. Agencies ask us today how we are going to cut costs in these areas by moving to the cloud.

The one cost that I think will be a little more difficult to measure, but will be a big cost savings, is the cost to deploy new capabilities. Agencies traditionally have metrics for what it takes to deploy new capabilities in legacy systems, but it's a softer thing to measure when you do that in the cloud. The data is there, we just have to come up with a better way of measuring it because it is such a paradigm shift from how it's been done in the past.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

Like anything else, determining ROI for the cloud needs to be measured against an accurate baseline. That's difficult for many traditional IT services because they weren't necessarily baselined in the past. Many of those services came from shadow organizations that carried their own facility and commodity costs such as utilities. Those costs probably were not factored into the baseline. So, when you look at that kind of situation, the cost of moving to the cloud can appear higher as most costs are now visible and you are paying for everything.

It's difficult to see where else agencies can accurately measure the effect of the cloud. They may be in an environment where reliability and performance are not good, for example, and so they are paying performance penalties whereas in the cloud they are not. It's challenging to come up with a metric you can use to determine how much money you are saving if you initially did not characterize all of those costs from a baseline perspective.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

A well-done private cloud infrastructure will result in a 66 percent reduction in operating expenses. If you look back a couple of years, the benchmark cost for a physical or virtual server was about \$18,000 a year; today it's \$6,000 or less for a server operating in a cloud-enabled infrastructure. Those are real dollars. So, you are freeing up large amounts of operating expense dollars, as well as eliminating the capital expense conundrum that the government is constantly struggling with.

If you correctly execute cloud enabled private infrastructure you will realize savings and have refreshment costs built in to help avoid capital expenditures. That's not to say you won't have to deal with some large scale enterprise resource planning system that may come down the pike. But if you are thoughtful about what may be a good candidate for a public cloud offering, you will have a clear strategy for modernizing and transforming all of your applications within your portfolio leveraging the cloud. And there it's the same; it will be 66 percent cheaper than it was to run legacy applications in a non-cloud environment.

Q15 How do companies such as yours need to operate in the current market? What do agencies expect of you?

Jay Mork

Senior Director of Advanced Programs, General Dynamics Advanced Information Systems

The technology actually creates a change in the value chain for how agencies acquire various capabilities. Now, the business model is changing to better support agencies moving to the cloud. One company provides the hardware, another the infrastructure, and so on. The cloud let's agencies take advantage of available technologies easily and quickly. They can now work with market-leading providers based on what they need in their cloud to support their mission.

While agencies may be using a new acquisition mode, what hasn't changed is our continued focus on providing mission capabilities to customers. Because we started to invest in the cloud five years ago, we have been able to become mission capability experts using the cloud and are actually building and testing cloud pilots, helping customers leverage the power of the cloud to better serve their users to achieve mission success.

Samuel Abbate

Vice President, Defense Enterprise Solutions, Northrop Grumman Corporation

Transforming to the cloud is not an easy evolution for most organizations. There are a myriad of complex people, process, and technology issues that are both intertwined and independent at the same time. Customers need a trusted and experienced partner that understands the subtleties and realities of what moving to the cloud, operating in the cloud, and ultimately becoming the cloud entails.

Northrop Grumman fully understands how to work alongside customers in an agile way, providing both pragmatic and expert guidance that is rooted in our own enterprise's cloud transformation, as well as dozens of customers across our industry. There is no such thing as a "one-size-fits-all" and customers fully expect their cloud partners to have a mature understanding of how evolving security, standards, governance, and technologies will impact their missions. Our experienced approach allows us to provide valuable insight that helps build an organization's confidence during its transformation to the cloud.

Chris Smith

U.S. Federal Chief Technology and Innovation Officer, Accenture Federal Services

Our federal clients want an ally who is looking out over the horizon while, at the same time, helping them navigate through all of the current requirements. Our federal clients trust Accenture to help them change the way that government works, because we work, think and contract differently. We are in there day-in, day-out with them. We have a deep understanding of how things operate and the critical importance of mission delivery. We bring subject matter expertise gained from working with multiple industries around the globe. We will continue to help our clients solve their most complex challenges.