Agencies are reaching for the cloud, making slow but steady progress toward delivering secure services and new applications in a faster, more cost effective way.

The government’s 2011 “cloud first” mandate along with pressure to consolidate data centers, save money and support new mobile applications are among the drivers propelling agencies toward cloud technology.

It’s not a question of “if” agencies will embrace the cloud, but when, according to speakers at an Oct. 16 event titled, “Strategies for Creating Cloud Builder Organizations Across Government.” The challenge for agencies is figuring out the best way to get there.

“It’s important to keep in mind that cloud is not a destination, it’s a journey,” said Stanley Tyliszczak, Staff Vice President for Technology Integration and Chief Engineer Chief Technology Office, General Dynamics Information Technology. “[What] we are seeing evolve now are the first steps of that journey.”

The journey to the cloud for agencies should begin with establishing a common, simplified infrastructure, based on open standards. “You need to have an architecture. You don’t get to the cloud by accident,” said Andy Ingram, Vice President, product marketing, Data Center Business Group, Juniper Networks.

The U.S. Customs and Border Protection, for instance, created a common delivery platform to serve as a commodity-based, horizontally-scalable, high-performing infrastructure.

“For us it was quite the culture change,” said Wolf Tombe, Chief Technology Officer, U.S. Customs and Border Protection, Department of Homeland Security. The common delivery platform became the foundation for how the agency built its infrastructure for its applications to run on. This approach allowed the agency to purchase its infrastructure as a service and rebrand the common delivery platform as common cloud environment.

Standardization is key to enabling automation, which makes it easy for users to provision services such as new networks and additional storage.
The benefit of cloud technology is that computing resources are provisioned as needed. However, many challenges in moving to the cloud are organizational, rather than technical, because of the siloed nature of many agencies, said Rob Randell, Director, Systems Engineering, NSBU, VMware. “It’s really important that there is top down initiative that forces these teams to start to work together.”

The Department of Health and Human Services, which has 12 operating divisions with different security needs, figured out how to integrate FedRamp into its security program by establishing the right team of people that shared a common goal: using cloud computing.

HHS developed its own FedRamp program to address the different security needs across the department, which wasn’t easy. “Our focus was keeping it to the baseline,” said Jennifer Gray, Chief, Service Design Branch (Acting), Office of Information Technology Infrastructure and Operations, Enterprise Engineering Division, HHS. Orchestrating an effective IT enterprise depends on bringing people together and ensuring the right technology and processes are in place, Gray said.

It also helps to ask the right questions up front in order to understand what users need and expect. What are the needs of the application owners? What is the right balance between security and access? What is the best cloud architecture or mix of architectures—private, public, hybrid or community—that fits the mission?

In moving to the cloud, start small, migrating small groups of users at a time and moving easy applications—such as email—to the cloud first. Agencies should also pay attention to the details of their cloud contract starting with agreeing with the vendor on the definition of cloud. The contract should also require FedRamp certification, along with auditing, monitoring, the ability to encrypt their own data, and software-defined networking.

Most cloud implementations in government so far have been private clouds, but this is changing. For instance, NSA is developing a community cloud for the intelligence community and the Department of Homeland Security has thrown its weight behind a national public safety community cloud.

Community clouds, if done right, are the most cost effective cloud architecture, Tombe said. The benefits are “huge and potentially transformative” as to how response teams would operate in a disaster.

You don’t get to the cloud by accident. You have to have a road map. You have to have an architecture.”

— Andy Ingram, Vice President, product marketing, Data Center Business Group, Juniper Networks
MEETING FEDERAL CLOUD EXPECTATIONS—WHAT’S POSSIBLE IN 2015 AND BEYOND

SPEAKER

Andy Ingram, Vice President, product marketing, Data Center Business Group, Juniper Networks

- The network is the foundation of the modern cloud.
- When building a cloud environment, organizations must start with a common architecture.
- A standardized, simplified infrastructure is easier to automate. Self-provisioning is a fundamental tenant of cloud automation.

SPEAKER

Rob Randell, Director, Systems Engineering, NSBU, VMWare

- The biggest challenge from a cloud perspective is organizational; the technology is there.
- Organizations must determine and closely manage who has access and control of the data in order to reduce risk.
- Standardization is key to enabling automation, which makes it easy for users to provision services such as new networks and additional storage.

SPEAKER

Stanley Tyliszczak, Staff Vice President for Technology Integration and Chief Engineer Chief Technology Office, General Dynamics Information Technology

- When migrating to the cloud, first understand what the needs of the application owners are, and then start small, migrating services such as e-mail first.
- Organizations need a cloud architecture that doesn’t have a single point of failure.
- Build and test a scenario in advance that can automatically reconfigure the network and reallocate resources in the event of a disaster.

SPEAKER

Chris Smith, Vice President, Technology, AT&T Government Solutions

- Cloud is the ability for low cost commodity compute to run huge workloads at a very low cost. The barrier of entry is gone.
- When considering the cloud, have a very clear vision of what workloads go where, realizing that some applications will remain in a legacy environment.
- In a multi-cloud environment, it helps to have multiple security models based on a certain standard.

SPEAKER

Michele Weslander Quaid, Chief Innovation Evangelist, Public Sector CTO, Google

- Move applications such as email and calendar to the cloud first; then identify applications that will be recoded for the cloud and those legacy applications that will stay in the data center.
- Choose a cloud provider that can offer containerization for microservices, support for open standards, instant replication, extensive auditing, no single point of failure and 100 percent uptime.

One of the great things about the cloud is this concept of automation and speed, but if you don’t start from a secure place you’re not going to have that.”

— Rob Randell, Director, Systems Engineering, NSBU, VMWare

It’s important to keep in mind that cloud is not a destination, it’s a journey. One of the things we are seeing evolve now are the first steps of that journey.”

— Stanley Tyliszczak, Staff Vice President for Technology Integration and Chief Engineer Chief Technology Office, General Dynamics Information Technology

We see (cloud) as an ecosystem of providers and these things working together ultimately that drives the biggest benefit for whatever mission you may be driving.”

— Chris Smith, Vice President, Technology, AT&T Government Solutions