

The Cloud and Government: The Next Wave

Presented to the SaasGov 2009 Conference

Daniel J. Chenok
Senior Vice President, Pragmatics
ChenokD@pragmatics.com

February 25, 2009

This Week's Headline

- “USA.gov will move to cloud computing” –
Federal Computer Week, Feb 23
 - Services via a cloud computing model where applications and data are delivered on the Internet
 - GSA expects to reduce its Web management costs by more than 50 percent
 - GSA officials also expect cloud computing to establish a foundation for a new generation of Web 2.0 and other online services.

The Context: Networks Reign

- Prelude:
 - Over 200 years of constitutional Government – many cultures, missions, institutions, communities
 - Only 15 years of e- Government – the network connects
- E-Government and technology innovation
 - Continuous expansion from mainframes and data matching to systems and data sharing to networks and data access
 - Distributed infrastructure, applications, data
- Networked architecture as the new paradigm
 - Cloud, Saas, Web 2.0, Social Networking
- Security and privacy are essential elements
 - ISPAB Cloud&Security Forum – csrc.nist.gov/groups/SMA/ispab

Distributed Everything

Citizens/Individuals – Social Networks		
Organizations – Professional Networks		
Networked Architecture	Enterprise Information Management	Web 2.0, Info Retrieval/Sharing Content, Records, Knowledge Management
	SOA-based Applications	SaaS, Web Services
	Distributed Infrastructure	Cloud, Grid, Virtualization

Innovative organizations and individuals embrace the network

Relevance

- Candidate Obama radically transformed the use of technology
- President-Elect Obama used Change.Gov to solicit innovation
 - Net neutrality was a key focus – helps ensure diversity of innovation
 - Broadband expansion enables consumer and small business use
 - Green agenda provides synergy
- President Obama signed Open Gov EO on Day One
 - Transparency, Participation, Collaboration – cloud promotes all
 - Innovation key to performance improvement (CTO, CPO)
- Fiscal realities demand radical cost savings with improved performance in agency computing platforms
- Cloud have proven effective in State governments
 - DC, Arizona State U, California Pub Utilities
- International competitiveness

Advantages for Government (sound familiar?)

- Cost savings across the lifecycle
- Flexibility
- Agility
- Responsiveness
- Mobility
- Innovation
- Resiliency
- Capacity optimization
- Promotes collaboration/shared developer and user communities
- Platform and application neutral

Taxonomy for Government

(adapted from Bill Whyman's presentation to ISPAB)

Application as a service

Applications offered directly to the user as a network service

On-demand apps (SaaS) refers primarily to the software applications & Internet services

– *Some E-Gov initiatives*

Computing as a service

Underlying IT resources (compute, storage, database) as a public network service

Cloud computing extends down into the underlying hardware, storage and *networking infrastructure*
-- *ITI LOB*

Tools to build own private cloud or prvt. outsource

Sell customers tools to build their own mini-cloud or manage it for them (remote or on-premise)

Many IT vendors are associating themselves with clouds. Most sell tools to help customers make their on-premise infrastructure more “cloud-like.”

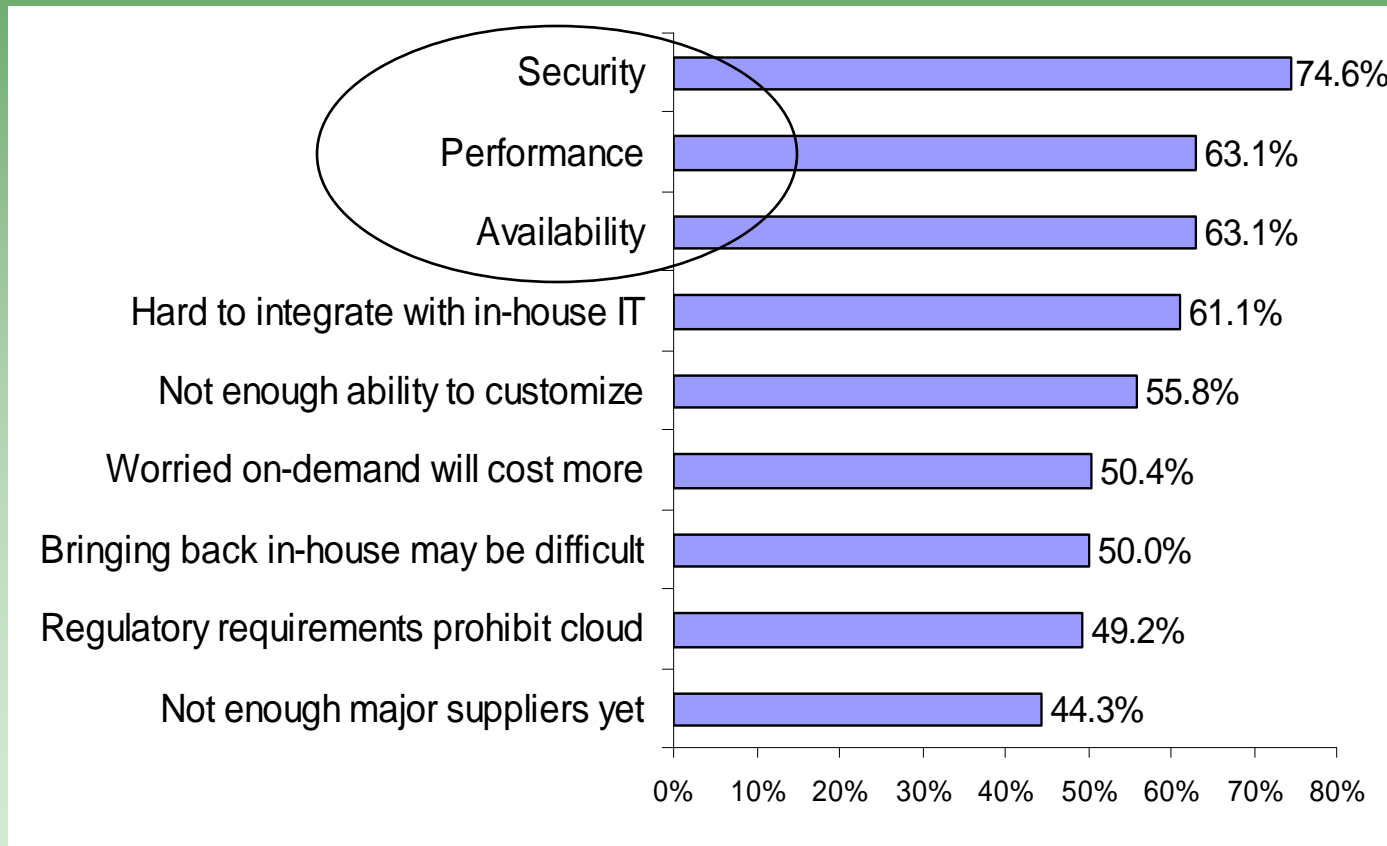
-- *Agencies ask for this, but does it optimize?*

Applications for the Cloud

- Cyber Network Protection
 - Sensor data storage, situational awareness
- Common Operating Picture to support military
 - Storage/processing of tactical intel feeds
 - Focus the view from different user roles
- Satellite Imagery – geospatial hosting
- Shared Software Development -- DISA
- Potential Implementation Models
 - Use of commercially provided cloud services
 - Deployment within networks (build their own)
 - Multi-agency Federated model
 - Hybrids

User Issues : Security, Performance, Availability

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model



Networked Security and Privacy

- Security – multiple needs
 - Governments and their missions
 - Industries and their roles
 - Academia, R&D
 - Users
 - Only a comprehensive strategy can accomplish balance
- Privacy
 - Breaches – real and perceived impacts
 - Particular issue for health IT and the cloud
 - Individual knowledge and control as the key
- Third Party Data
 - Individual control
 - Liability

Some Security Challenges

- General risks
 - Protection of sensitive data, regulatory compliance, data location, data segregation, recovery
- FISMA compliance – systems v. networks
- Security of applications riding on the cloud
 - Ensure confidentiality, integrity, availability
 - Controlling what applications can run on which platforms
- Protecting cloud platforms from cyber attack – new challenge or opportunity?

Issues for the Future

- Data Ownership implications
 - What happens when something goes wrong on a cloud server?
 - Law Enforcement access to personal information in the cloud
- Stovepipes v. standards – interfaces are key
 - NIST: set a common architecture
- Legacy integration will bring significant challenges
- Loss of control requires change management
- Records Management a unique issue for agencies
- Contracting needs to adjust – change from purchase to subscription model
- New kinds of IT governance issues goes away – more lateral management to match distributed networks

Possible Approaches Moving Forward

- Options:
 - 3rd party clouds for non- sensitive data
 - procure a single USG cloud
 - procure multiple independent non-interoperable USG clouds
 - work towards a Federal cloud infrastructure (standards and architecture)
- NIST working on special pub

Questions?