



Information in the Cloud: What's in the Future

**“Cloud Computing: Opportunities, Advantages,
Disadvantages for Federal Agencies”**

Melvin Greer

Chief Strategist, Author, Educator

SOA / Cloud Computing / Cyber Security

July 2010

About Me:

LOCKHEED MARTIN



Senior Fellow

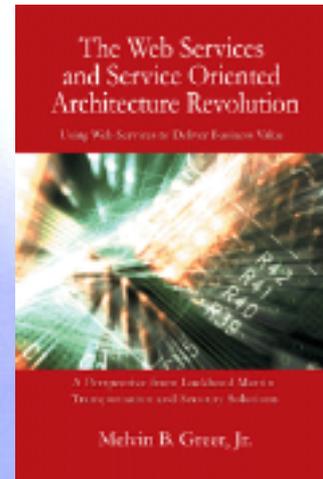


Professor / Distinguished Lecturer

Practitioner



Author



computing

service
operating provider often
future or demand
without designed
multiple many real

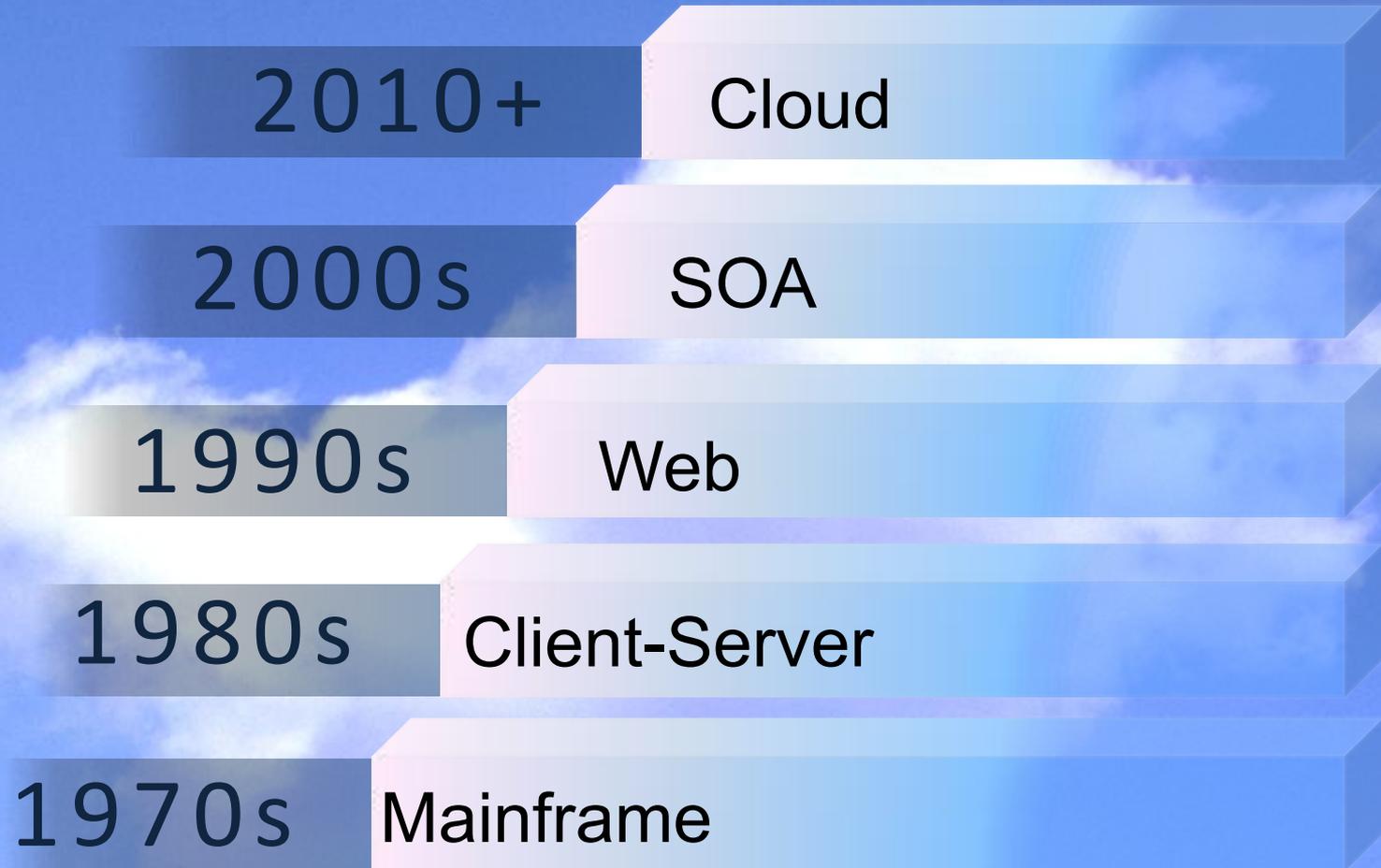
software
resources
systems
Google
capital network
basis
also
data
web applications
edit
architecture
Users
customers
control
expenditure
virtual storage
physical
might
term
networks
applications
physical
might
term
networks

cloud

application system
Private cost
computer
Internet
Amazon
Microsoft
servers
SaaS
management
electricity
Retrieved
delivery
and/or
hardware
client
Microsoft
fine-grained

business
time
access
used
work

The next big thing?



You are the Cloud



Gmail™



hulu™



facebook



twitter



You Tube
Broadcast Yourself™



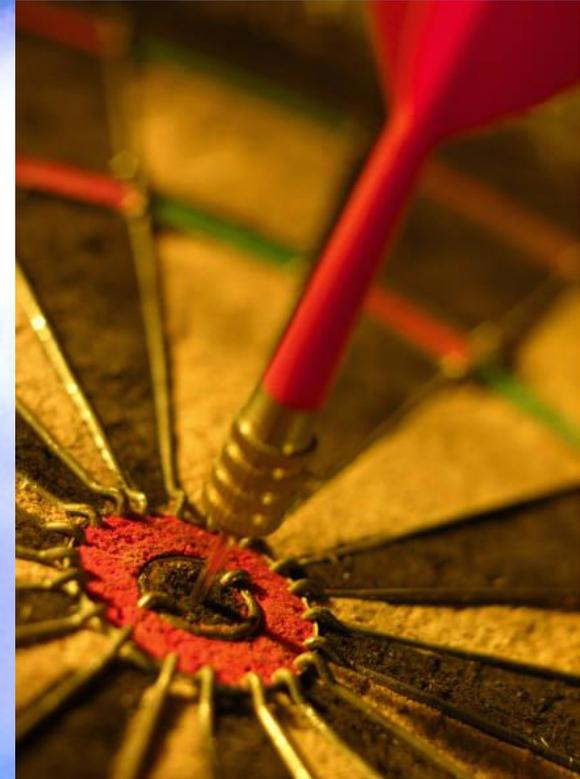
Linked in®

amazon.com®



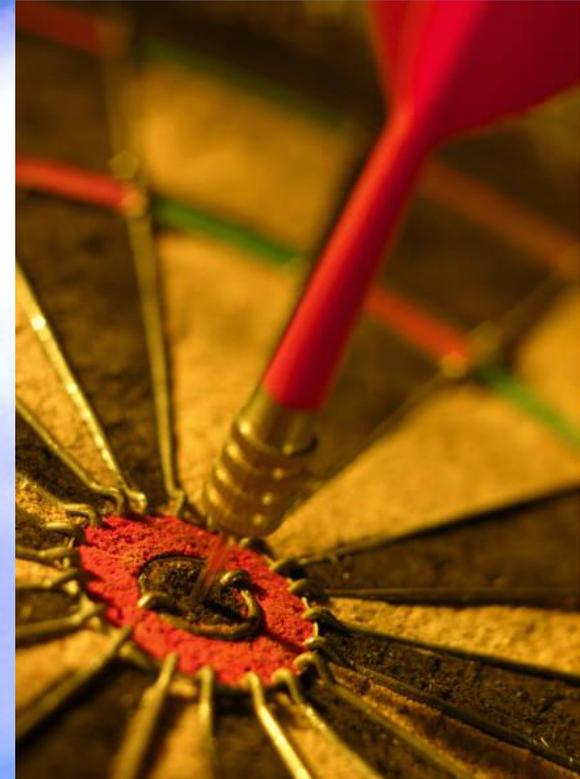
Key Issues

- What Trends will accelerate the Government shift to Cloud computing?
- What is Cloud Computing
- What are specific technical considerations for Federal Cloud Computing?
- How do we re-think our security architecture given Cloud risks and threats?
- What is the future of Federal Cloud Computing?



Key Issues

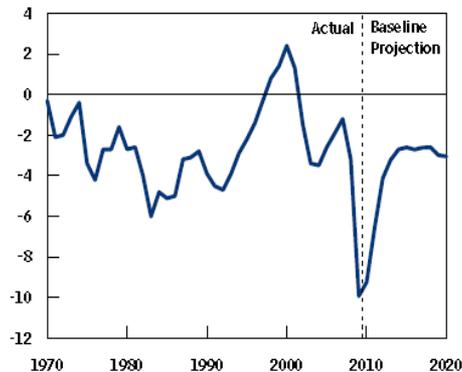
- **What Trends will accelerate the Government shift to Cloud computing?**
- What is Cloud Computing?
- What are specific technical considerations for Federal Cloud Computing?
- How do we re-think our security architecture given Cloud risks and threats?
- What is the future of Federal Cloud Computing?



Trends

Record Setting U.S Federal Budget Deficit – \$1.6 Trillion

U.S. Federal Budget As a Percentage of GDP



Source: Congressional Budget Office.

Constrained Future Federal IT Spend

- **Budget Freeze** would take effect in October 2010 and limit the overall budget for agencies to \$447 billion a year
- White House is directing Agencies **trim** their **budget by 5%**. Agencies are directed to **freeze discretionary spending** except in National Security

Cloud Adoption Implications

- The “new normal” for Federal Agencies is **constrained budgets amid pending budget freezes to reign in mammoth budget deficits**
 - Deliver more with less
 - Extreme Transparency
- **Need to reduce capital and on-going expenditures**
 - OMB halting some new projects
 - Cloud option required (e.g. Data Center Consolidation Initiative)
- **The overriding driver for Cloud Computing will be the economic case that reduces cost and increases performance**
 - In addition to the core economic comparison, risk will be a major criteria to balance the economic case

Trends

Experiential Understanding of Cloud Computing



Every professional discipline impacted by the Cloud

- **Every Day activities** depend on use of cloud computing
- **Mobile devices** are the primary entry point into the cloud

Cloud Adoption Implications

- **Ease of use, access, performance and price expectations are set**
 - On demand, ubiquitous
- **Cloud Specific Business Models**
 - Consumption based pricing
- **Speed and Agility of Mobile apps**
 - Two way design and development

Trends

Increased comfort putting PII Data in the Cloud



Life in a Fish Bowl

Convenience over privacy

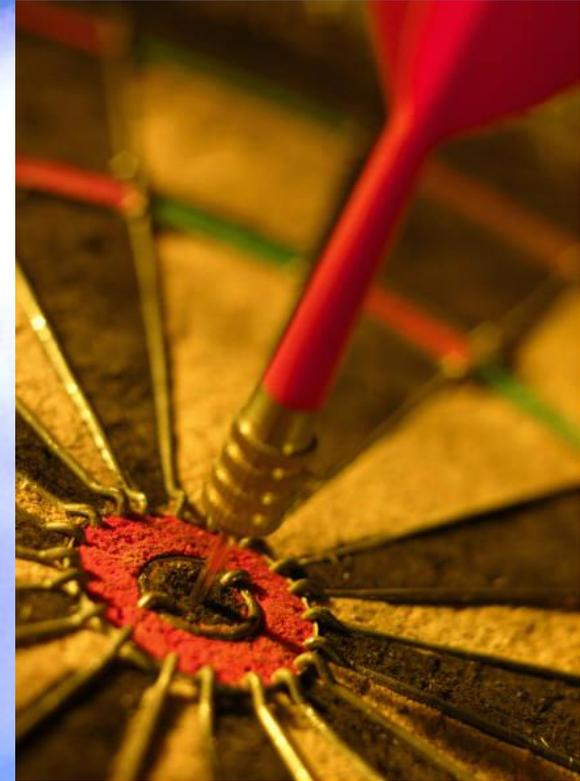
- **No detail** is too private
- **Major convenience** is traded for increased access to data

Cloud Adoption Implications

- **Data is the oxygen to cloud computing**
 - Data drives cloud development
- **Massive, permanent data storage**
 - Customized, tailored solutions
- **Business Intelligence and Analytics**
 - The Business of Data

Key Issues

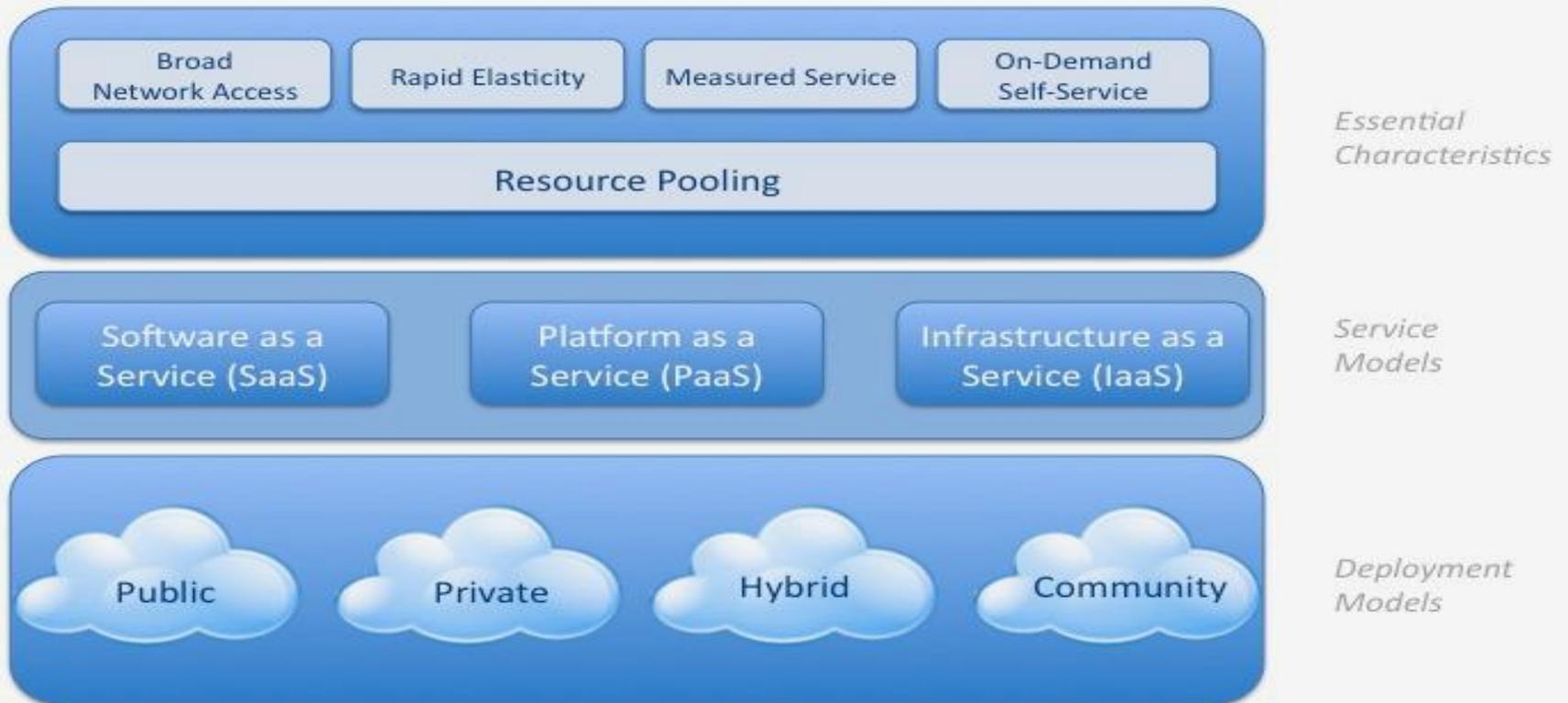
- What Trends will accelerate the Government shift to Cloud computing?
- **What is Cloud Computing?**
- What are specific technical considerations for Federal cloud Computing?
- How do we re-think our security architecture given Cloud risks and threats/
- What is the future of Federal Cloud Computing?



Definition

Visual Model Of NIST Working Definition Of Cloud Computing

<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>



Definition – Key Characteristics (NIST)

① On-demand self service



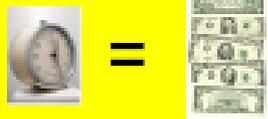
renting takes minutes

② Ubiquitous network access



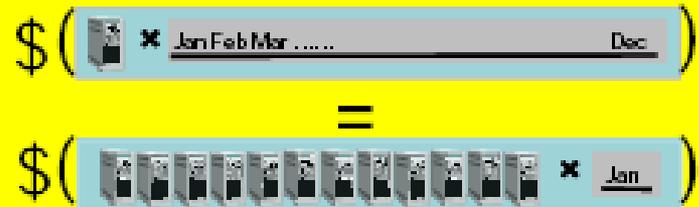
anywhere / any device

③ Metered use



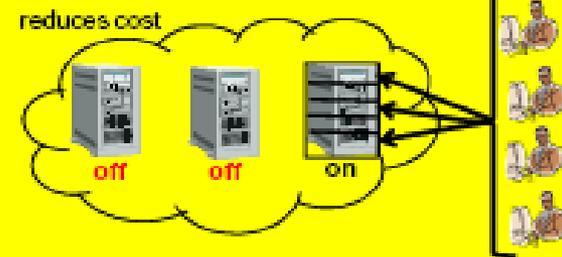
conserve resources

④ Elasticity

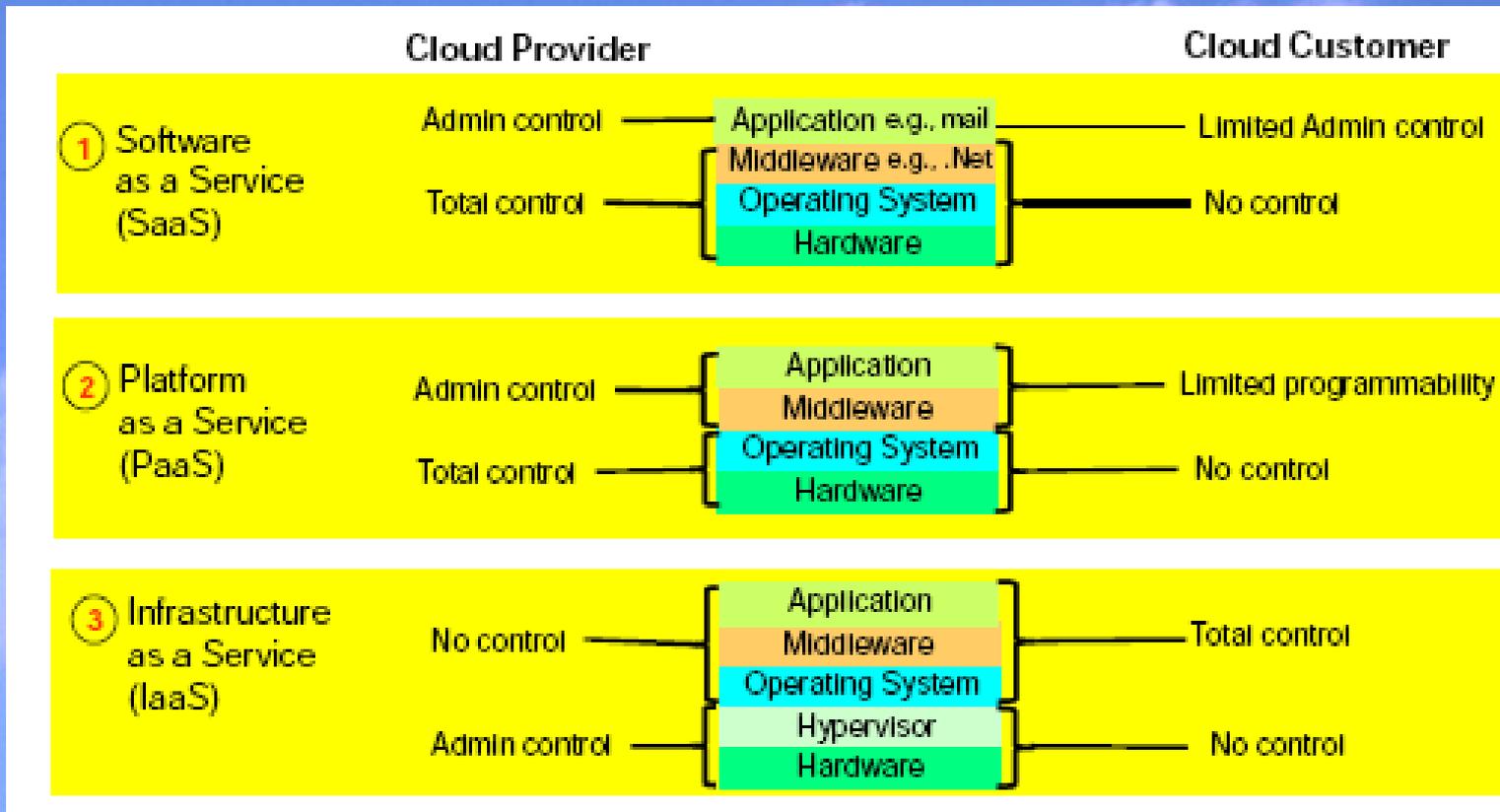


rent it in any quantity

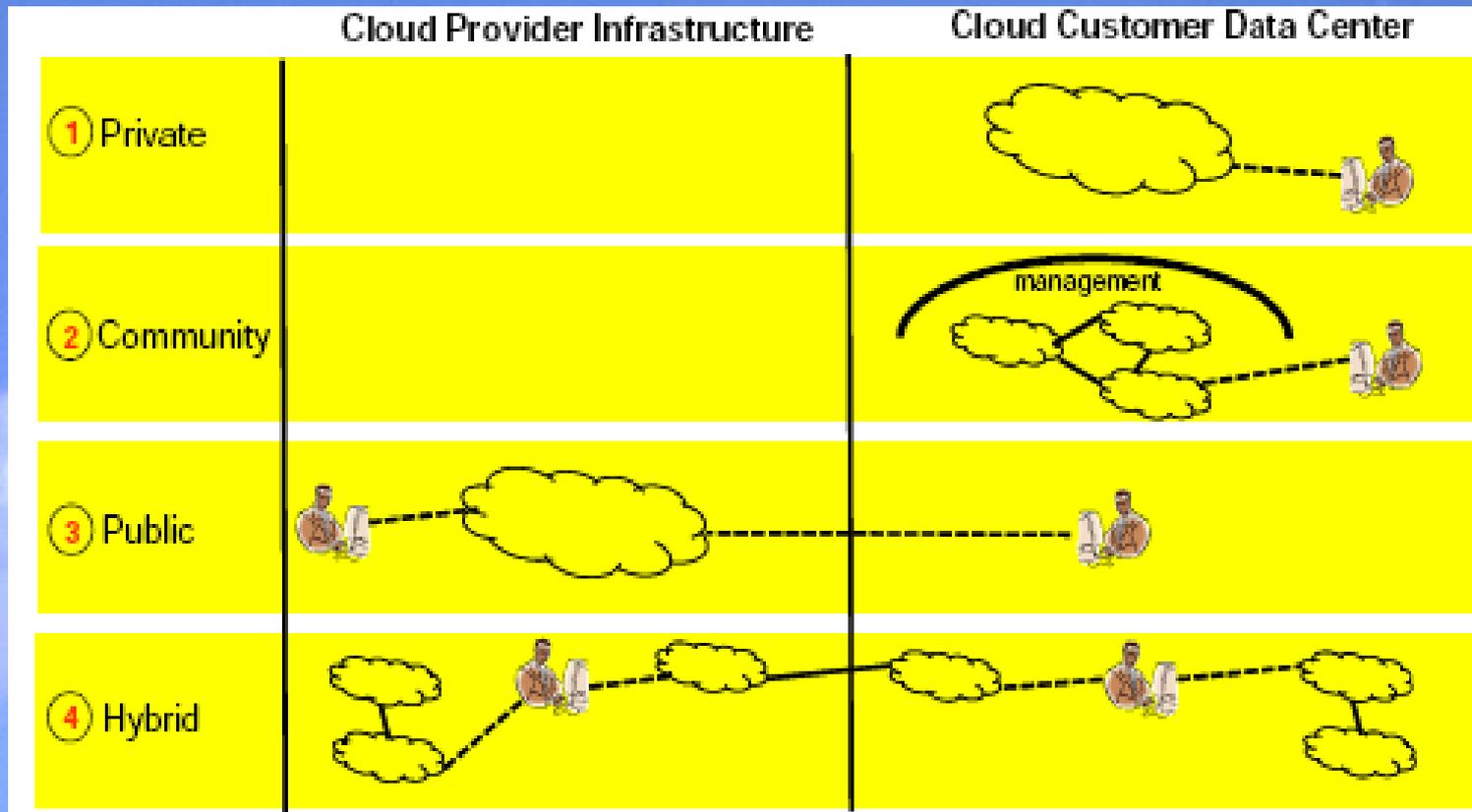
⑤ Resource pooling



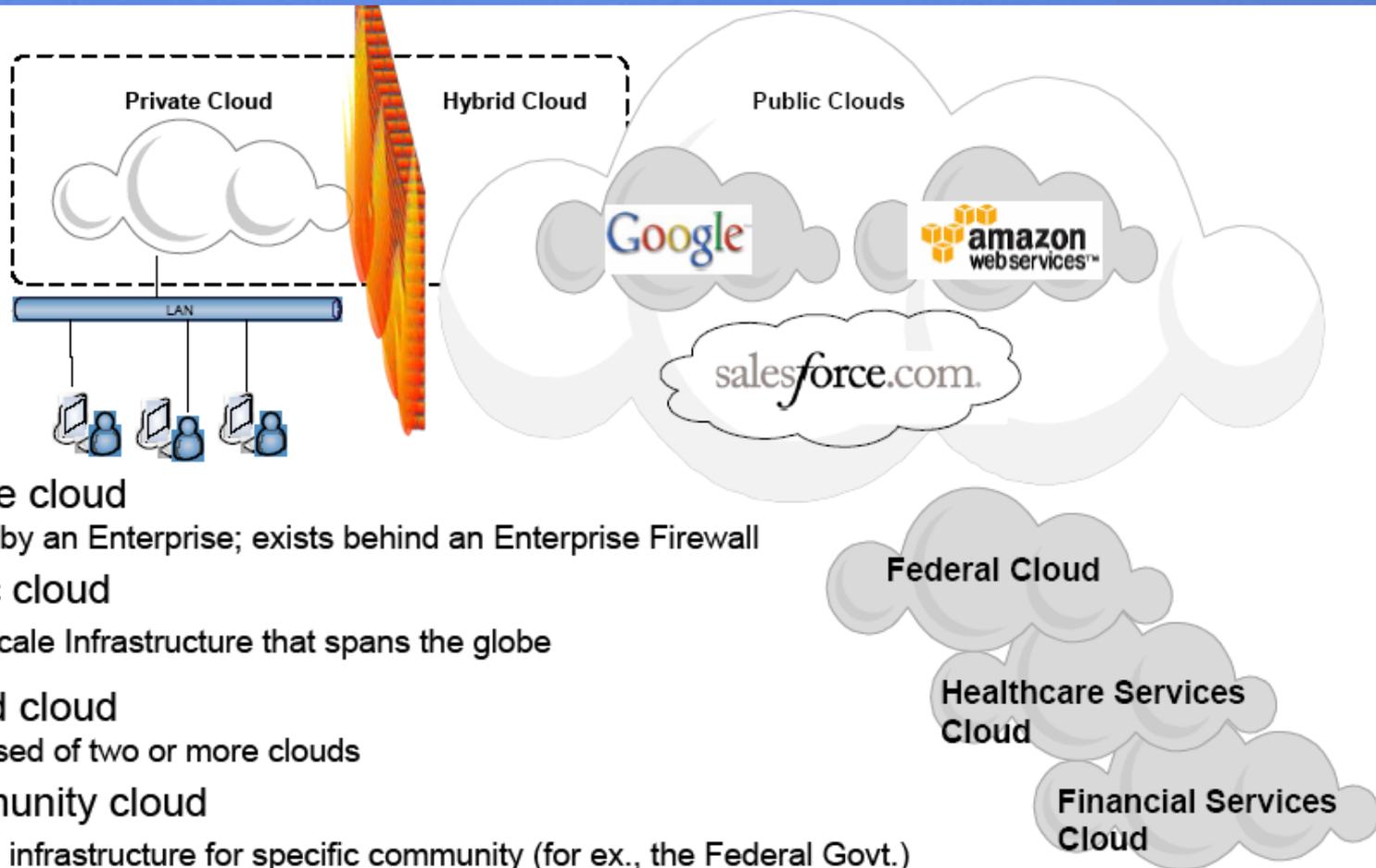
Definitions – Deployment Models (NIST)



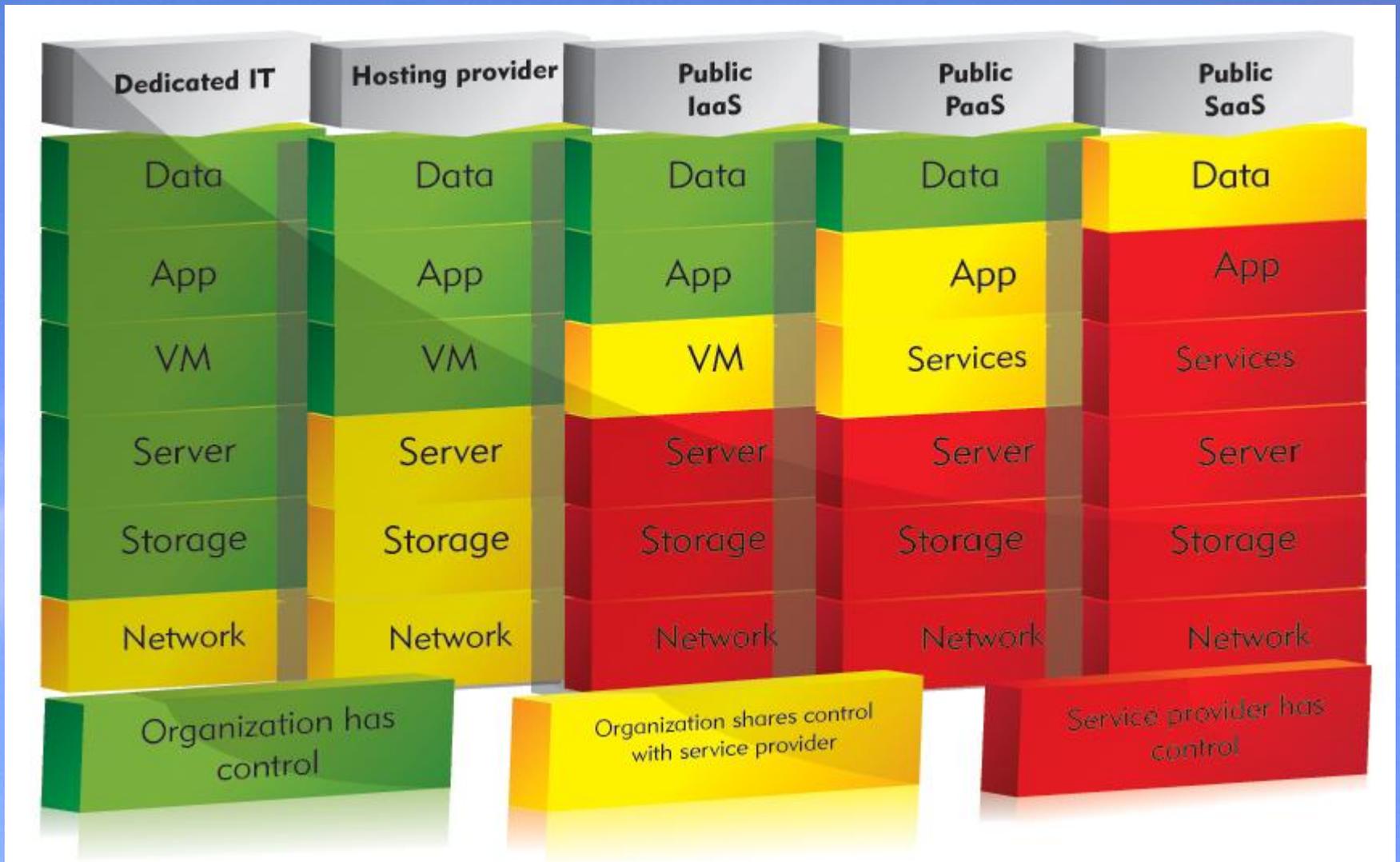
Definitions – Delivery Models (NIST)



Cloud Computing Concept Architecture



Data Control



Strategic on-ramp to Advanced Software

Lightweight
Programming



Javascript + XML

Rich User
Experience



Networking

Web as Platform



Locations

Data as the
Discriminator



Auctions

Software
Transcends the
Device



iPOD

Harness
Collective
Intelligence



Online Encyclopedia

Non-traditional
Release Cycles

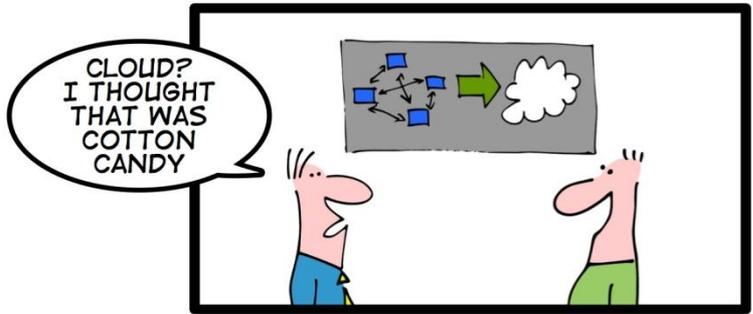
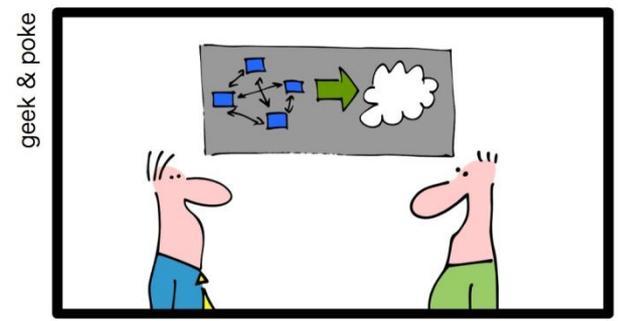
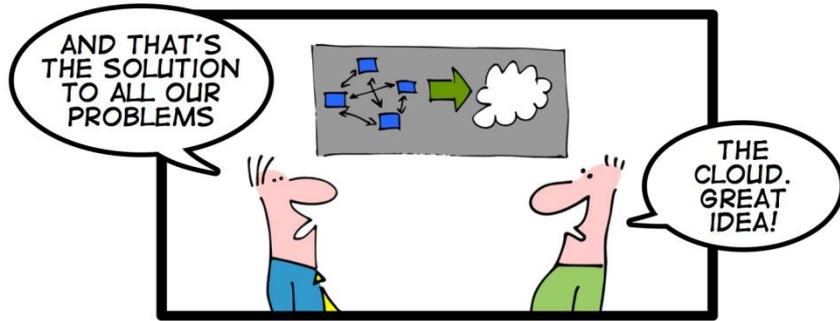


Photos

Cloud computing Concept



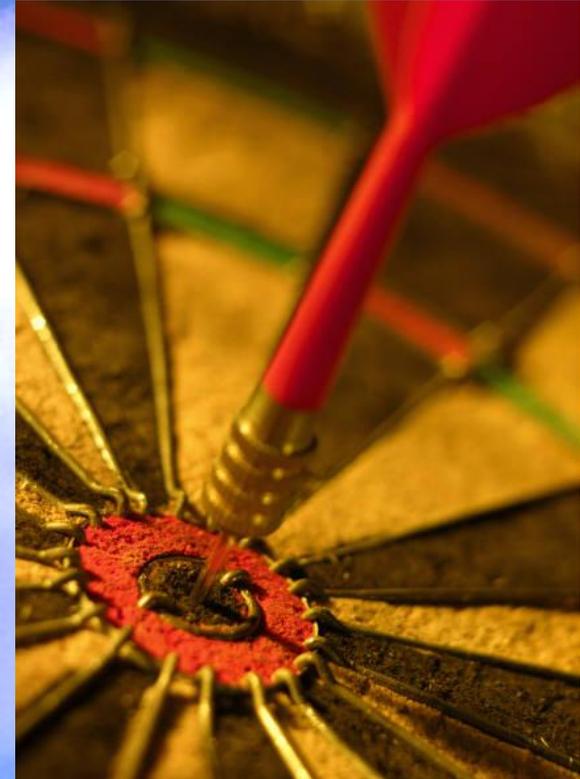
On-demand, scalable, elastic service



CEOs LOVE THE CLOUD

Key Issues

- What Trends will accelerate the Government shift to Cloud computing?
- What is Cloud Computing?
- **What are specific technical considerations for Federal Cloud Computing?**
- How do we re-think our security architecture given Cloud risks and threats?
- What is the future of Federal Cloud Computing?



Presidents Guidance

“The Federal technology environment requires a fundamental reexamination of investments in technology infrastructure.”

“The Infrastructure Modernization Program will be taking on new challenges and responsibilities. Pilot projects will be implemented to offer an opportunity to utilize more fully and broadly departmental and agency architectures to identify enterprise-wide common services and solutions with a new emphasis on cloud computing. “

“The Federal Government will transform its Information Technology Infrastructure by virtualizing data centers, consolidating data centers and operations, and **ultimately adopting a cloud-computing business model.**”

FY2010 Federal Budget

Analytical Perspectives

Cross Cutting Programs

<http://www.whitehouse.gov/omb/budget/fy2010/assets/crosscutting.pdf>

Cloud Computing in the Federal Government

- FEMA added Twitter to the national emergency response network
- Census Bureau using Salesforce.com to manage activities partner organizations
- Web 2.0 A-Space: An award winning
- SaaS application for intelligence
- Apps for Army, Army Private Cloud
- National Geo-Spatial Agency Community Cloud
- National Institutes of Health iPhone Apps



Cloud Computing Technical Considerations



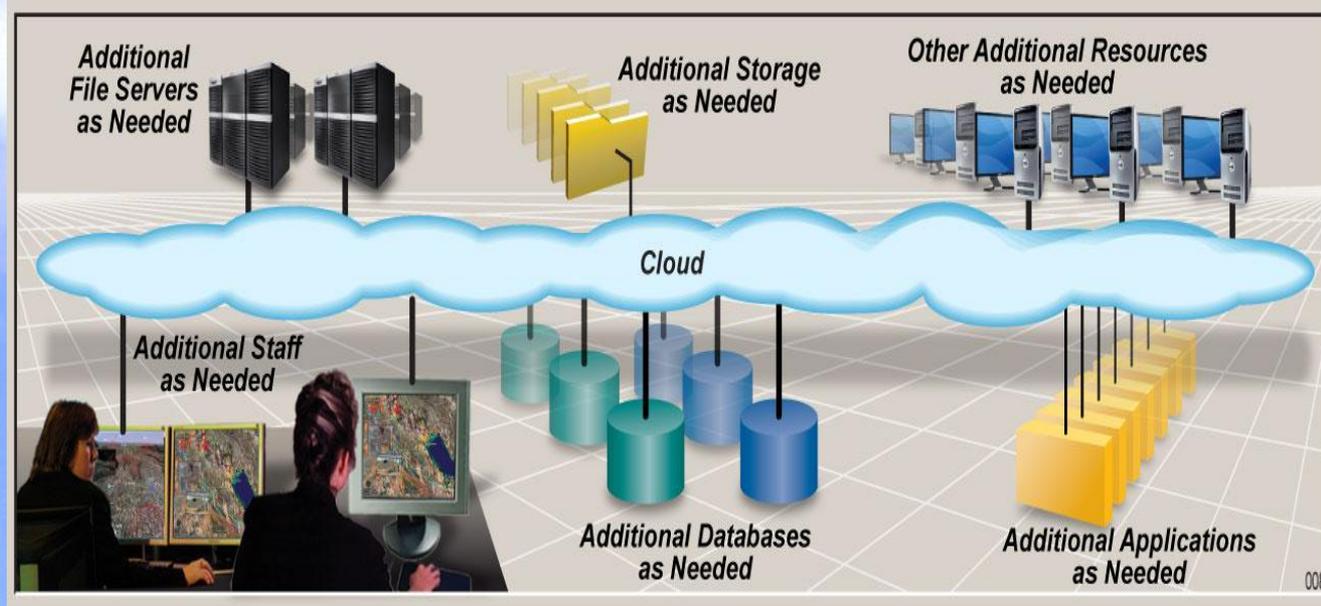
Cloud Computing Technical Considerations

- 1) **Planning and Requirements**
- 2) **Architecture and Design**
- 3) **Development**
- 4) **Testing and Integration**
- 5) **Operations and Maintenance**



Cloud Computing Technical Considerations

- 1) *Planning and Requirements*
- 2) **Architecture and Design**
- 3) *Development*
- 4) *Testing and Integration*
- 5) *Operations and Maintenance*



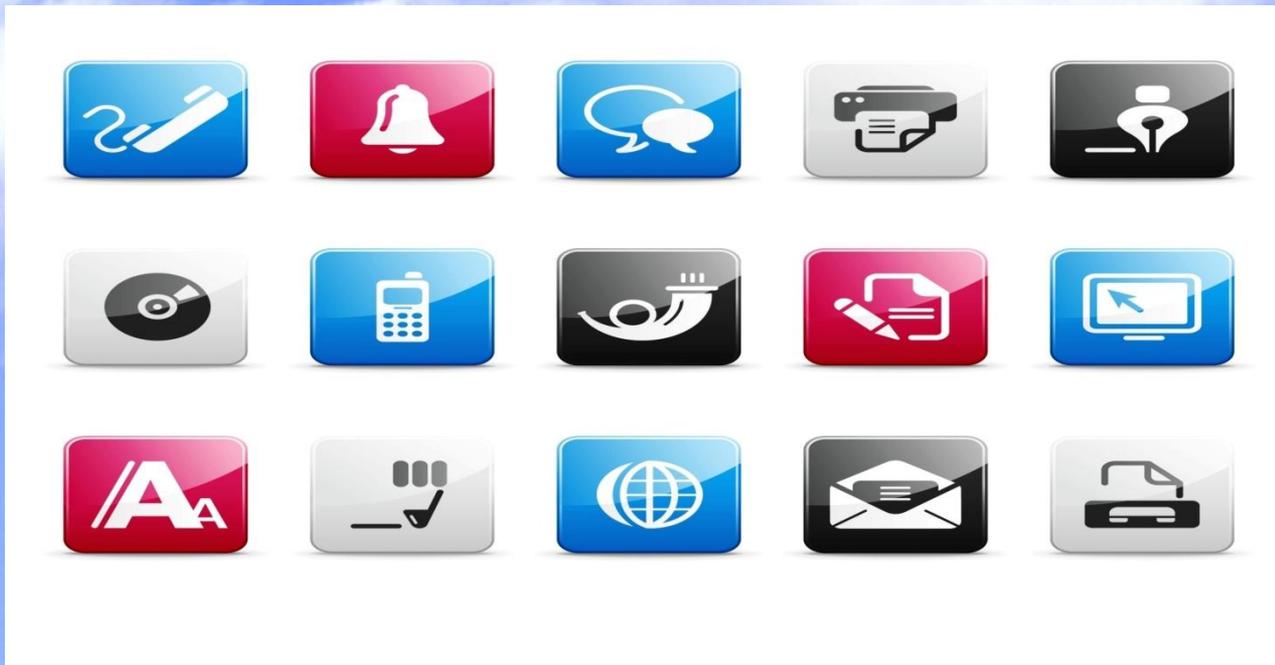
Cloud Computing Technical Considerations

- 1) Planning and Requirements*
- 2) Architecture and Design*
- 3) Development**
- 4) Testing and Integration*
- 5) Operations and Maintenance*



Cloud Computing Technical Considerations

- 1) *Planning and Requirements*
- 2) *Architecture and Design*
- 3) *Development*
- 4) **Testing and Integration**
- 5) *Operations and Maintenance*



Cloud Computing Technical Considerations

- 1) Planning and Requirements*
- 2) Architecture and Design*
- 3) Development*
- 4) Testing and Integration*
- 5) Operations and Maintenance***

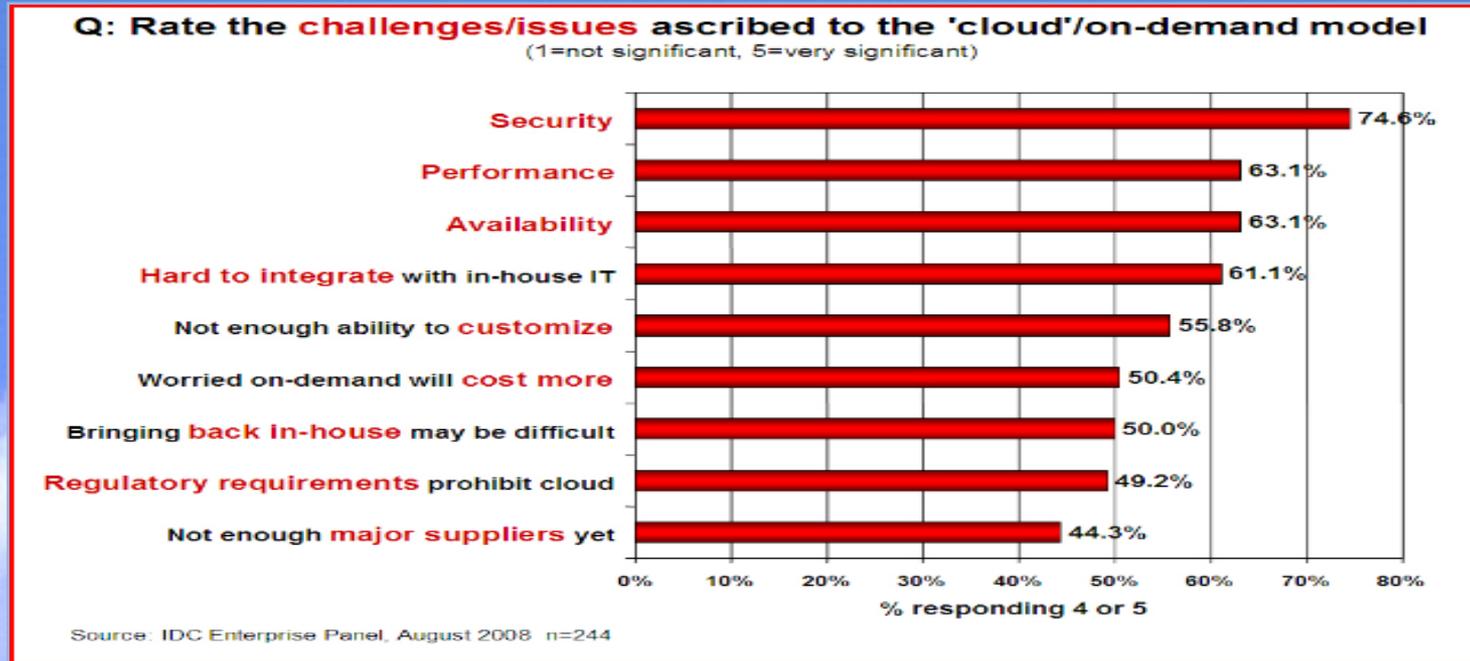


Key Issues

- What Trends will accelerate the Government shift to Cloud computing?
- What is Cloud Computing?
- **What are specific technical considerations?**
- **How do we re-think our security architecture given Cloud risks and threats?**
- What is the future of Federal Cloud Computing?



Challenges and Risks



Although government IT organizations are showing an increasing interest in cloud computing, they are also concerned about risks in areas such as data privacy, access and security.

Security Risks

- Public cloud's multi-tenant, dynamic characteristics may put sensitive, or regulated data at risk
- Vendor viability creates strategic risk
- Denial of service attacks could create systemic risk
- A lack of transparency and accountability about security from cloud vendors lowers trust



The Cloud is Made of Software
Attacks that leverage the software's environment, services and systems the software relies on, and communication channels it uses to communicate all take on new magnitude in the cloud

Legal, Financial and Reputational Risks

Personally identifiable information (PII), classified, or export-controlled information going to the wrong country, making an organization responsible for the data's being noncompliant with national privacy or secrecy regulations

Contractual obligations for information separation or licensing being violated

Sensitive information being lost or damaged or suffering impeded access

Sensitive information unnecessarily released to legal process by a provider leading to a loss of Fourth Amendment protection (in the United States) against search and seizure

Legal exposure due to degraded ability to manage or search data in the cloud for e-discovery purposes

Liability if facilities are compromised and used as attack bots or spam bots or to aid/abet other harmful activities against third-party targets

Lawsuits or penalties from a cloud vendor for violating service agreements

Cloud Security Incidents

November 2007: [Salesforce Staff Speared by Phishers](#)

July, 2008 [Hey Spammers, Get Off My Cloud!](#)

March 2009: [Google Privacy Blunder Shares Your Docs...](#)

June 2009: [Webhost hack wipes out data for 100,000 sites](#)

October 2009: [Amazon Web Services DDoS Attack And The Cloud](#)

More at

<http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents Database>

Rethinking Security Architecture

Activities and data move across open, untrusted networks

Zoning must become more logical than physical

Tightly coupled domain access control must give way standards-based identity services

Security management and service-oriented architecture must support hybrid clouds

Encryption performance and key management must evolve to enable secure, cloud-based storage

Choices around authentication and access control, encryption algorithms, and policies around private data must be revisited

Security vs. Privacy and Confidentiality

Security: freedom from danger, risk, etc.; safety.

Privacy: The state of being free from unsanctioned intrusion

Confidential: spoken, written, acted on, etc., in strict privacy or secrecy, information, the unauthorized disclosure of which poses a threat



Cloud Provider Risk Mitigation

Cloud providers will

Security

- storage
- control
- access
- movement

have to demonstrate, and perhaps constantly certify, their security capabilities

Recovery

- replication

provide assurance that data and applications are replicated across multiple sites to reduce vulnerability

E-Discovery

- Audit
- Transparency

support internal investigations as well as legal or administrative electronic discovery requests



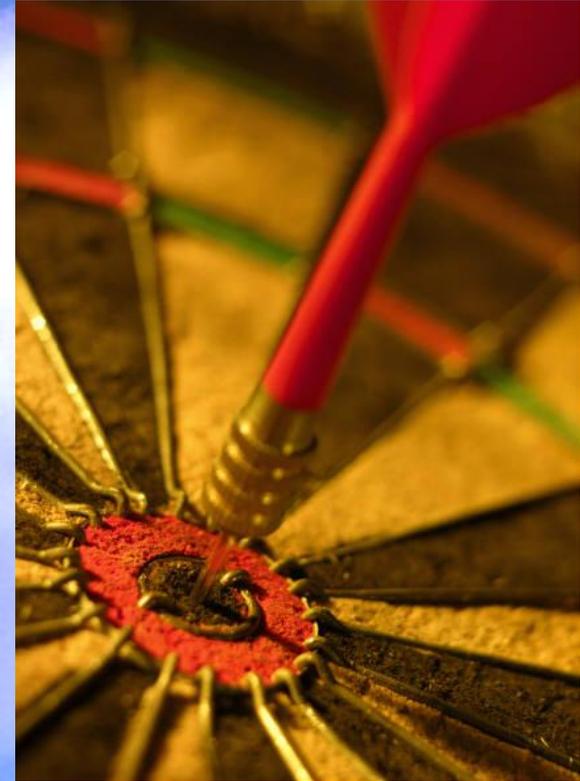
Cloud Consumer Risk Mitigation

- Beware of "ad hoc" cloud computing. Agencies should have standardized rules in place telling employees when and if they may utilize cloud computing and for what data.
- Don't put anything in the cloud you wouldn't want a competitor, your government, or another government to see.
- Read the Terms of Service. Then read the Terms of Service again.
- Make sure that you are not violating any law or policy, by putting data in the cloud, and think twice before putting any consumer data in the cloud.
- Consult with your technical, security or corporate governance advisors about the advisability of putting data in the cloud.

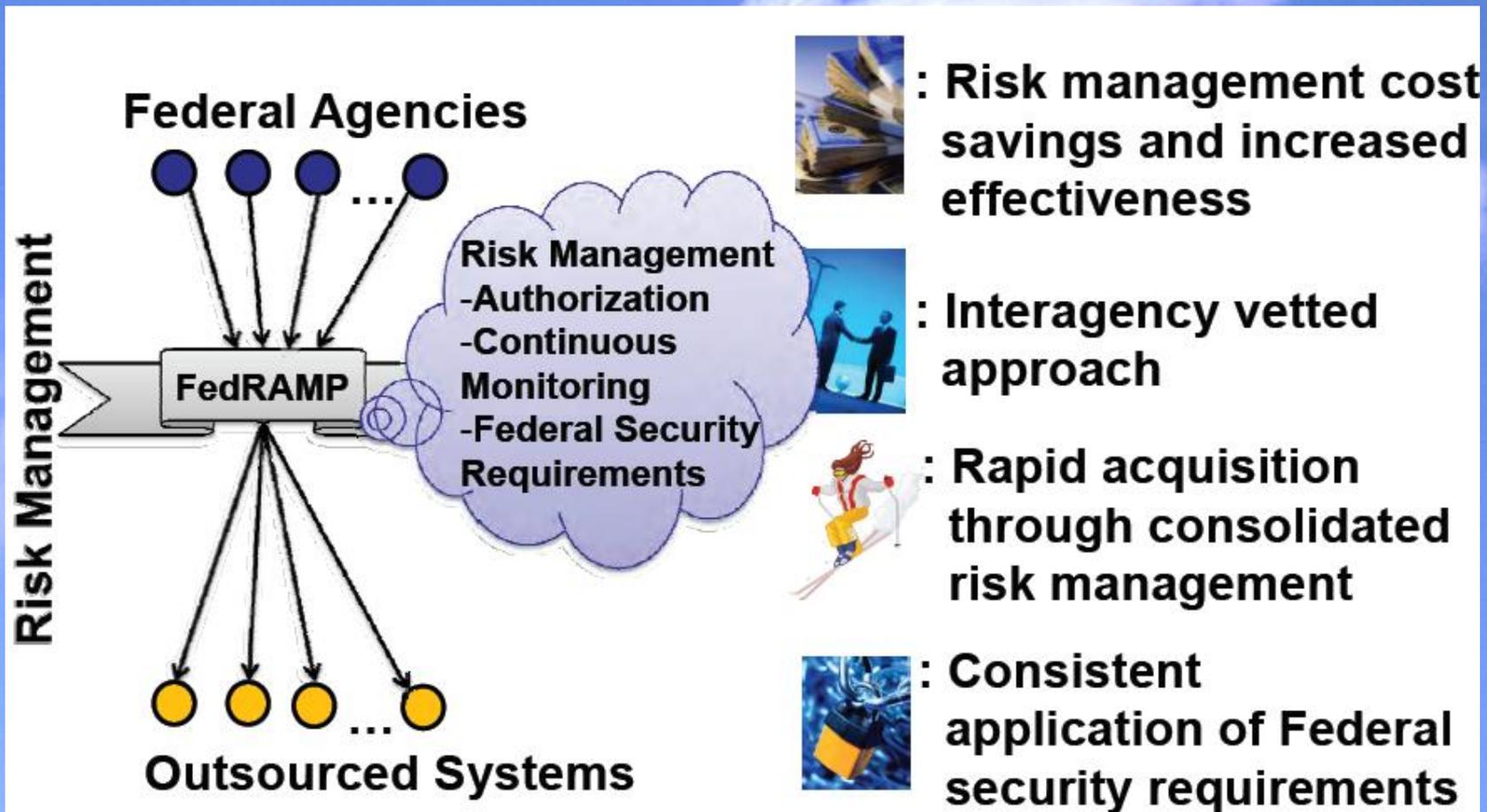
The executive and judicial branches have repeatedly taken the position that data stored in the cloud does not have the same assumptions of privacy and due process as does data stored in your own infrastructure – *ACLU report on Cloud Computing and privacy*

Key Issues

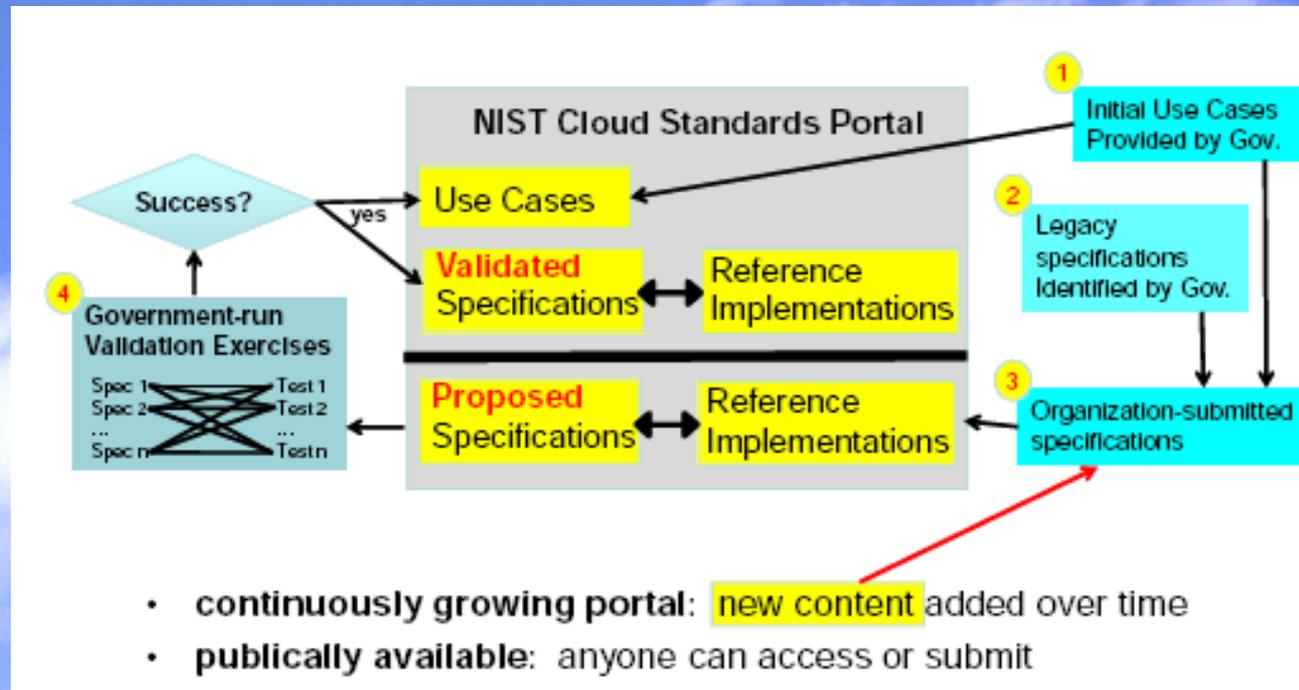
- What Trends will accelerate the Government shift to Cloud computing?
- What is Cloud Computing?
- **What are specific technical considerations?**
- **How do we re-think our security architecture given Cloud risks and threats?**
- **What is the future of Federal Cloud Computing?**



Federal Risk and Authorization Program

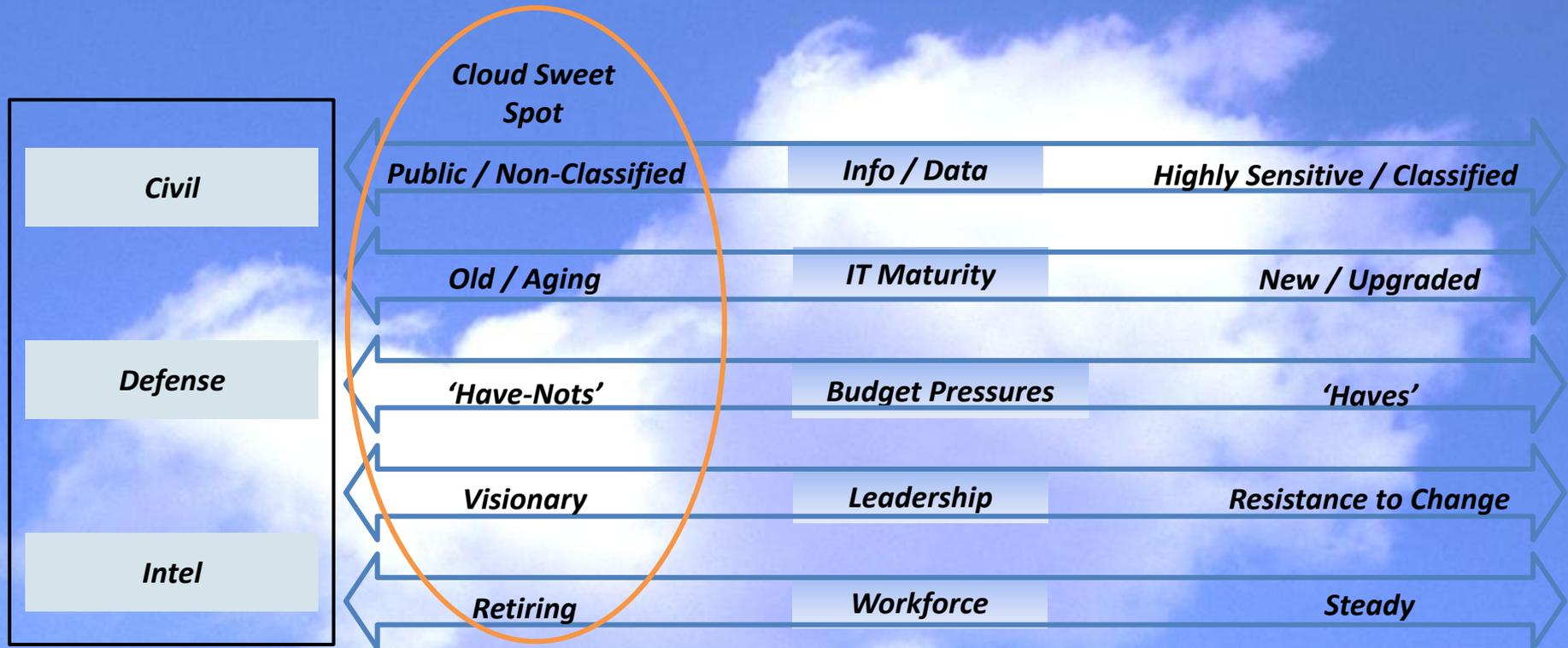


Standards Acceleration Jumpstarting Adoption of Cloud Computing (SAJAAC)

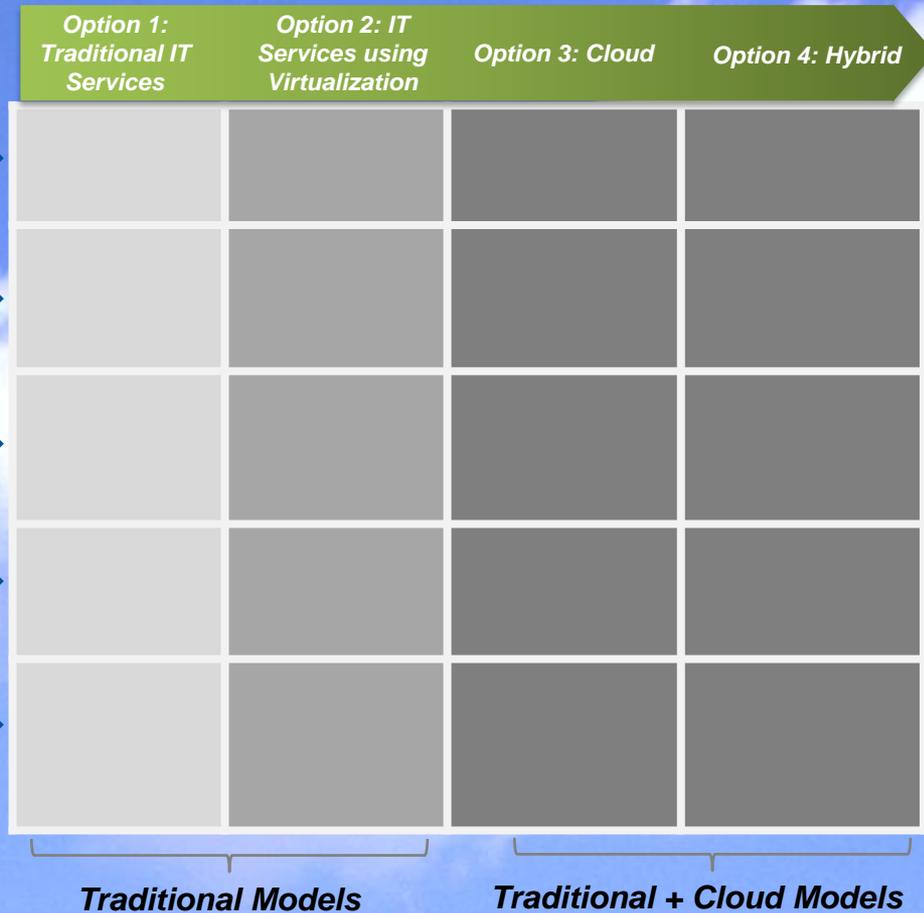


Community developed Cloud technical specifications and reference implementations

The More Dynamic The Environment, The Better Candidate For Cloud



Cloud Computing; An Alternative Sourcing / Delivery Model Against Traditional Models



Cloud Adoption Implications

- Agency decision makers will evaluate Cloud against other sourcing and delivery options
- Cloud options will need to address business / technical requirements but also provide improvement of cost / value
- Cloud is likely to be considered as a piece of the solution rather than the entire solution
 - This will create 'hybrid' environments where both Cloud and traditional IT services will co-exist

End User Driven with a focus on Data Portability and Cloud Interoperability



Melvin Greer
Chief Strategist, SOA/Cloud Computing
Lockheed Martin
Email: melvin.greer@lmco.com

Disclaimer: the views expressed in this PowerPoint presentation are the author's alone, and do not necessarily represent the official view of any component or institution with which he is affiliated.

