The NIST Cloud Computing Program

Robert Bohn
Information Technology Laboratory
National Institute of Standards and Technology

October 12, 2011

NIST National Institute of Standards and Technology U.S. Department of Commerce

Overview

- Background on NIST
- NIST's Role in Cloud Computing for the USG
- NIST Roadmap Efforts in Cloud Computing
- SAJACC – Inception, principles, activities
- Reference Architecture

NIST: Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

©Robert Rathe

Why NIST?

- US government agencies need Cloud Computing **standards & guidance** to accelerate effective adoption
- Private sector and U.S. government agencies must work together to identify highest priority USG Cloud Computing **security**, **interoperability**, & **portability** requirements & gaps
- **Neutral, objective** party is instrumental in encouraging innovation & "a level playing field" for U.S. industry

NIST Cloud Computing Program Goal

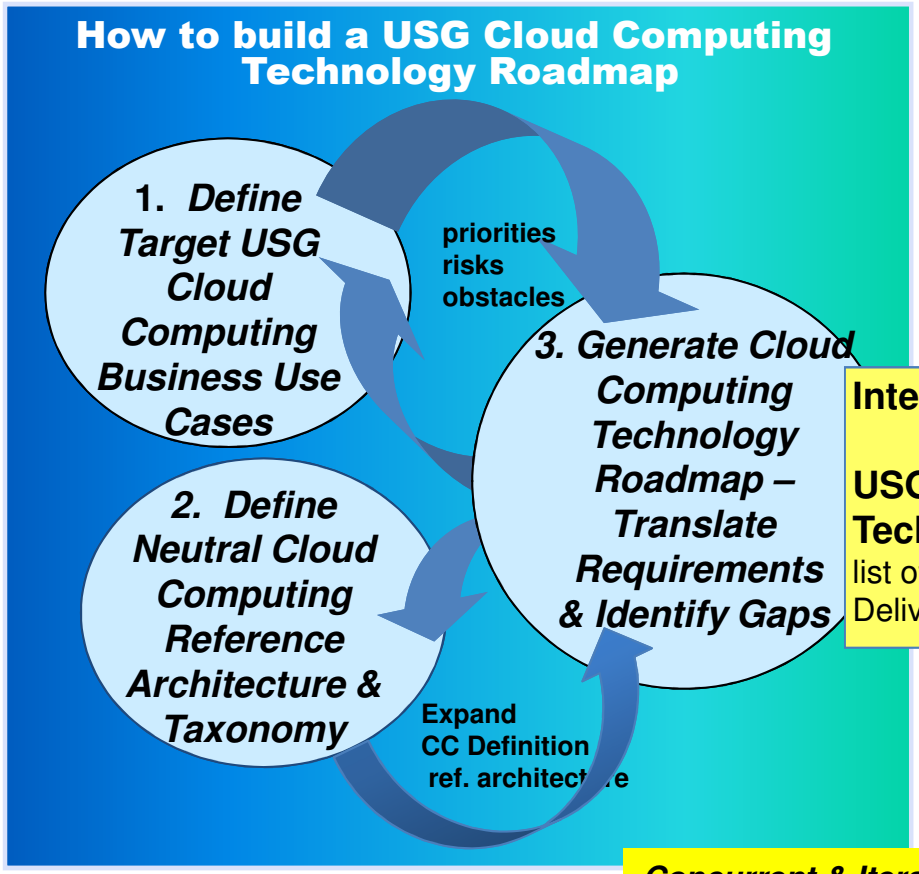
The NIST Cloud Computing Program and initiative to build a *USG Cloud Computing Technology Roadmap* is one of several complementary and parallel U.S. government cloud computing initiatives defined in the broader Federal Cloud Computing Strategy, February 2011

Accelerate the federal government's adoption of cloud computing

- Build a USG Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements
- Lead efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders

NIST Cloud Computing Program Concept

Strategic Program



Interagency Report:

USG Cloud Computing Technology Roadmap
list of Tactical Priorities & Deliverables

Concurrent & Iterative 3-step process that drives tactical efforts

Tactical Program

NIST CC efforts

- **Standards Working Group, SDO liaison, submissions**
- **Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC)** – through qualitative testing of specifications against interoperability, security, and portability requirements
- **Guidance –** Special Publications; technical advisor to Fed CIO Council (FedRAMP); Cloud Security Working Groups
- **Complex Computing Simulation & Modeling** – Koala IaaS resource allocation algorithms

NIST USG Cloud Computing Technology Roadmap: Content Expectations

General Content:

• present Exemplar Business Use Cases

• describe a conceptual model Cloud Computing Reference Architecture and Taxonomy

• identify existing interoperability, portability, and security standards and guidance that are applicable (or likely to be applicable)

• specify high-priority gaps for which new or revised standards, guidance and technology need to be developed (ie. 4 NIST SPs on cloud)

• document recommended action plans with aggressive timelines as candidates for self-tasking by participating government and private sector organizations

The content will include, reference and reflect work and products that are currently available through the NIST Cloud Computing public web site

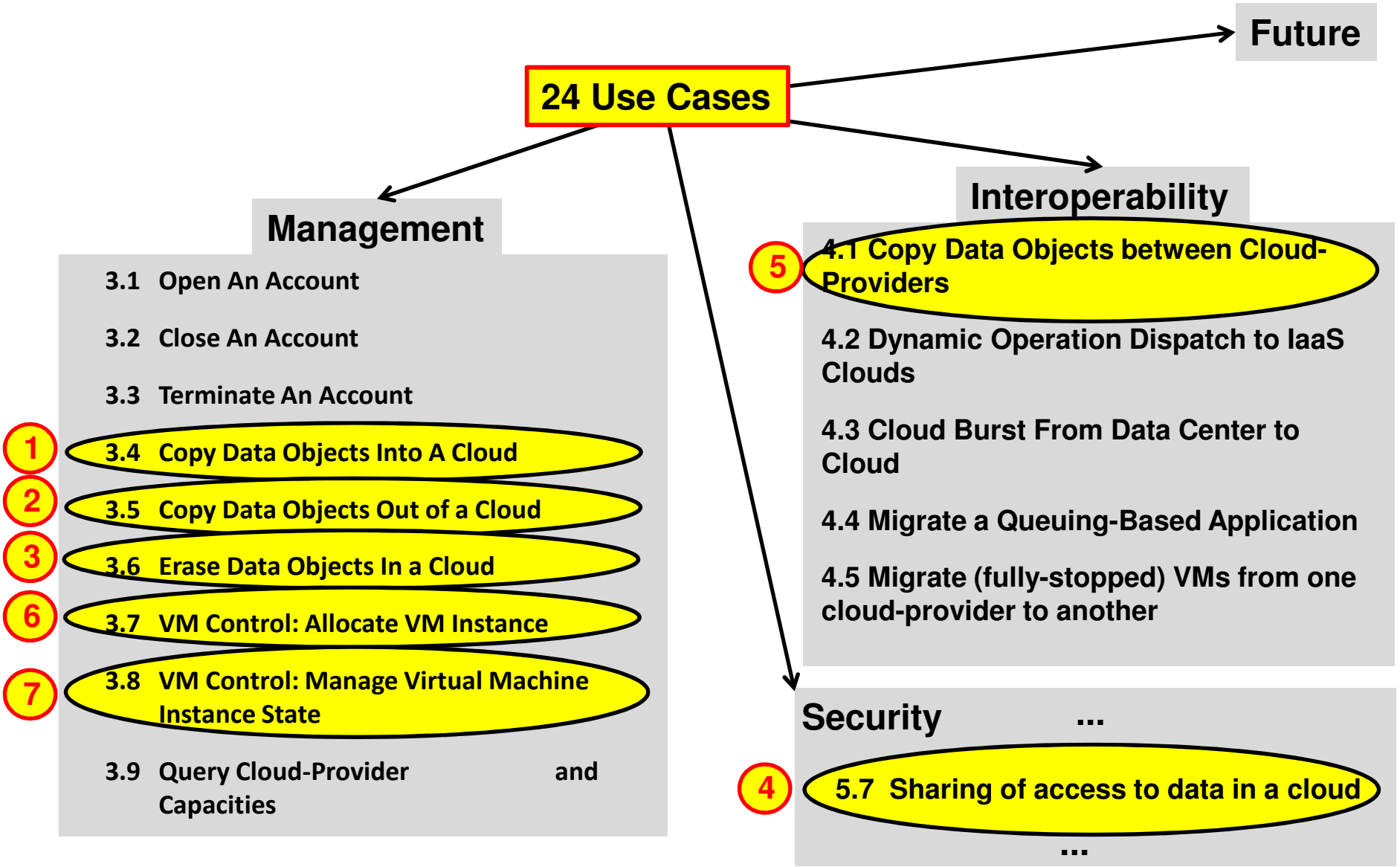
Tactical Effort: SAJACC
Standards Acceleration to Jumpstart the Adoption of Cloud Computing

Develop and maintain use cases (currently 24) through an open process with the goal of highlighting interoperability, portability, security

Collect and generate cloud system interfaces through an open process.

Develop tests showing how interfaces can satisfy use cases.

Prioritized Use Cases



A Few Observations

- No open support for direct cross-cloud copy (that we can find).
- Cloud-to-cloud implementations of common interfaces not widely deployed.
- Assured Cloud "Data Erase" appears to be problematic.
- For data object and VM management, different clouds sometimes have quite similar core features.
- Federated identity management may facilitate cloud interoperability.
- Subtle differences (e.g., timing) in similar (or almost identical) interfaces limits portability.

Plan Going Forward

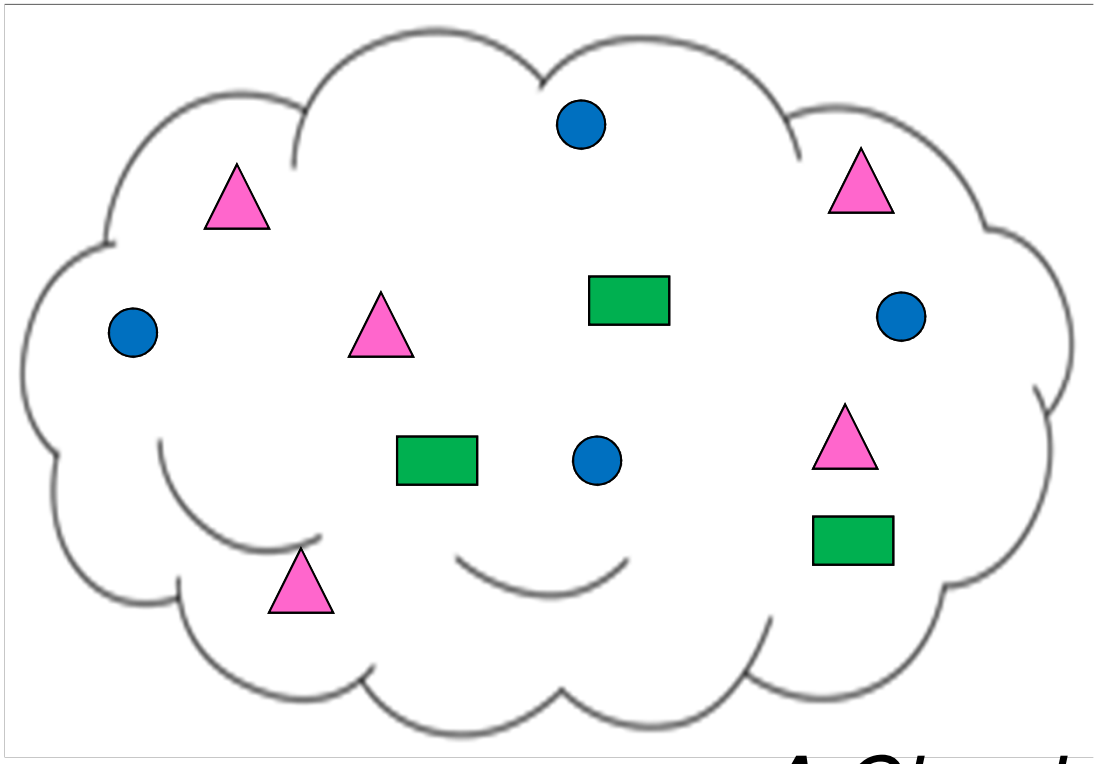
- Implement more use cases
  - Refine the Use Cases
  - Version 2 of the Use Case Document
- Cloud Interoperability focus
  - e.g., VM migration, identity management
- Encompass more of the available interfaces
- Expand the test driver infrastructure

Strategic Effort: Reference Architecture & Taxonomy

Service Models
-Software as a Service (SaaS)
-Platform as a Service (PaaS)
-Infrastructure as a Service (IaaS)

Deployment Models
-Public
-Private
-Community
-Hybrid

Essential Characteristics
-On demand self-service
-Broad network access
-Resource Pooling
-Rapid Elasticity
-Measured Service



A Cloud

Reference Architecture and Taxonomy Working Group

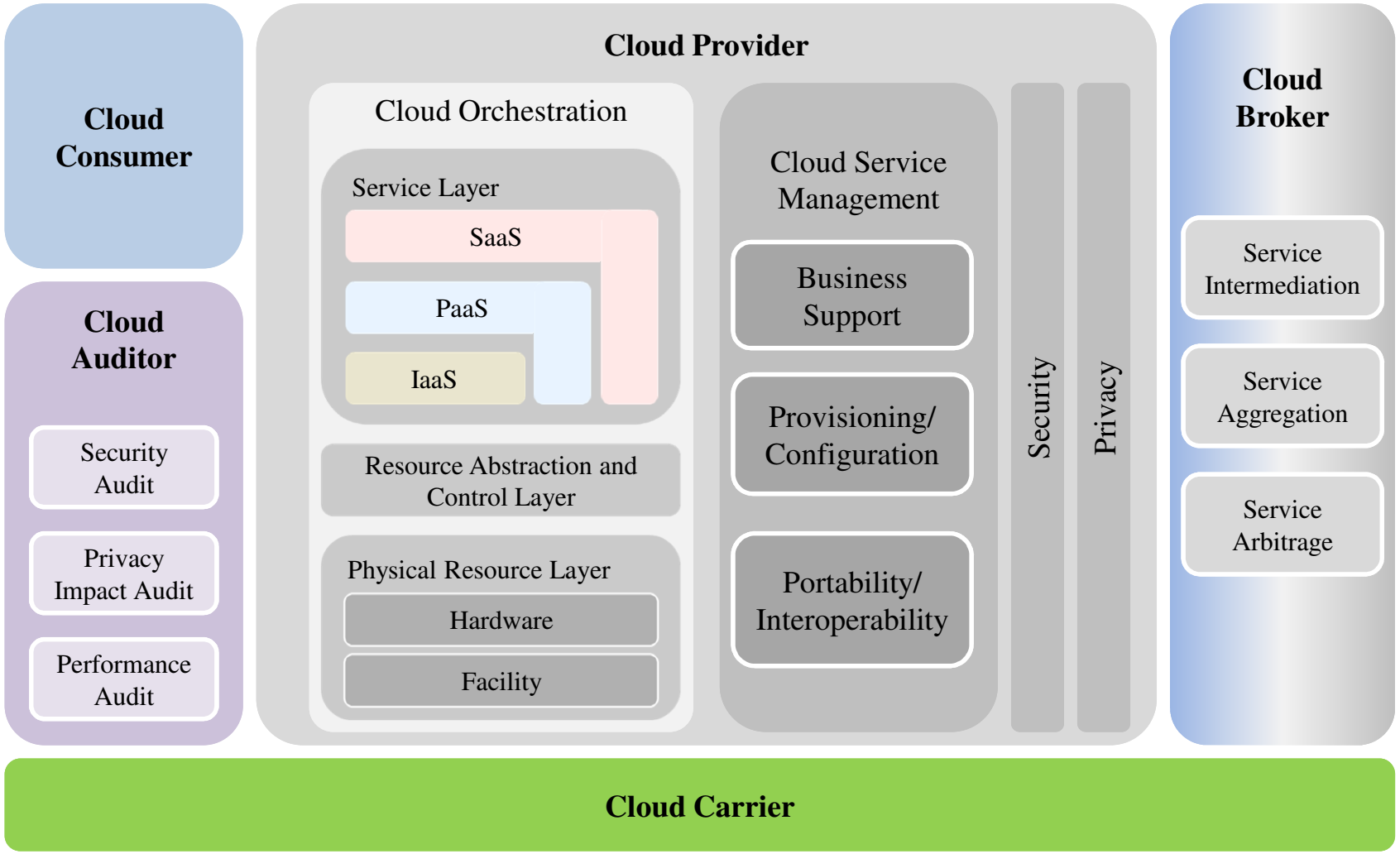
Goals: lead interested USG agencies and industry to define a neutral cloud computing reference architecture and taxonomy to extend the NIST cloud computing model to:

- use as a frame of reference to facilitate communication
- to illustrate and understand various cloud services in the context of an overall cloud computing model
- use as a tool to communicate and analyze candidate security, interoperability, and portability candidate standards and reference implementations

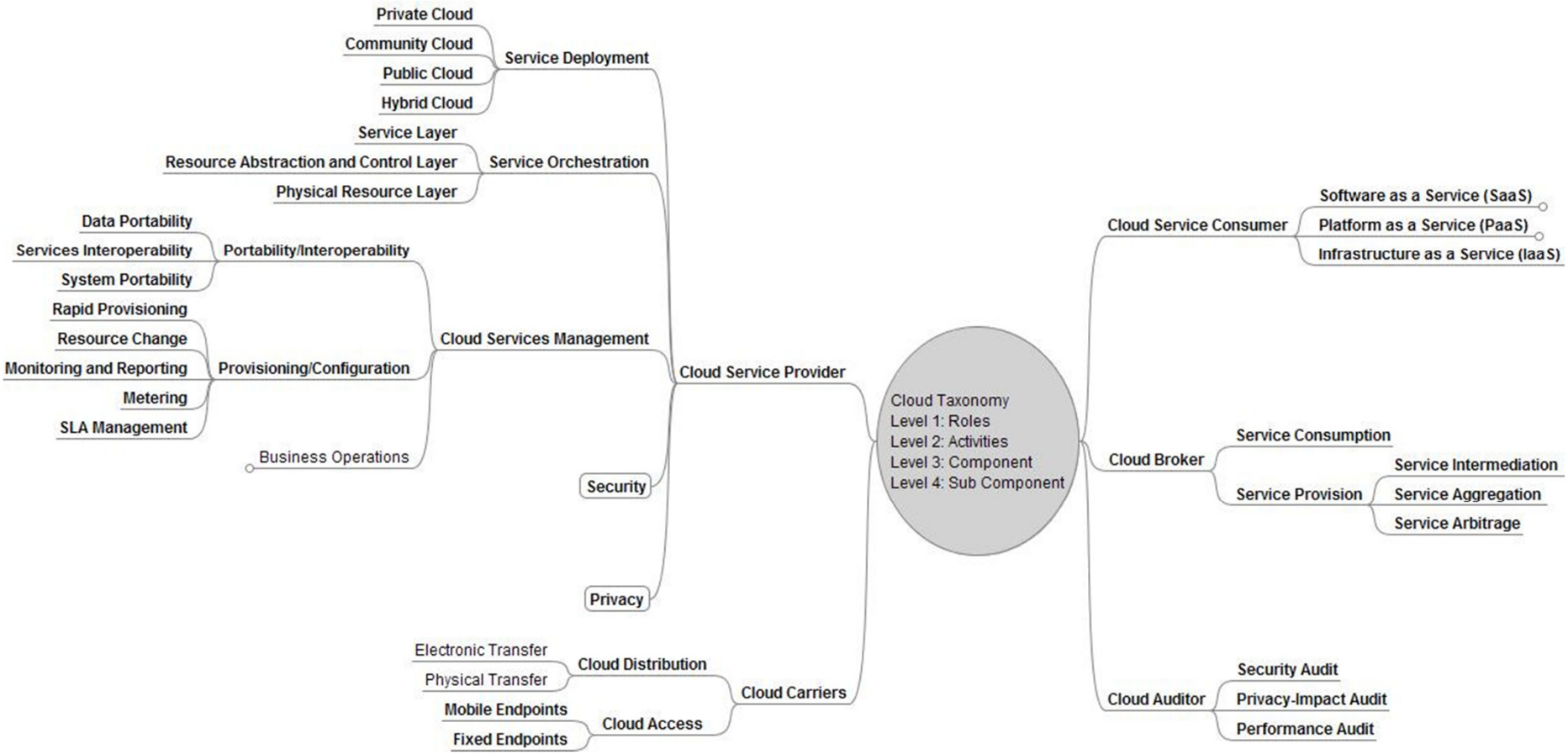
Process: The Working Group will leverage the existing, publicly available work, plus the work of the other NIST Working Groups, to develop a NIST Cloud Computing Roadmap that can be incorporated into the USG Cloud Computing Roadmap.

Output: NIST SP500-292 Cloud Computing Reference Architecture

The NIST Cloud Computing Reference Architecture



RA Taxonomy / Mindmap



Questions?

NIST Cloud Computing Collaboration Site

http://collaborate.nist.gov/twiki-cloud-computing/

NIST Cloud Computing Home Page

http://www.nist.gov/itl/cloud

Contact:

Dawn Leaf dawn.leaf@nist.gov
Robert Bohn robert.bohn@nist.gov
John Messina john.messina@nist.gov

Backup Slides

NIST At A Glance

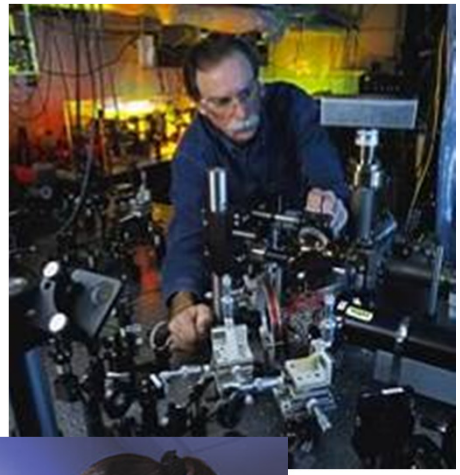
Major Assets

~ 2,900 employees

~ 2600 associates and facilities users

~ 1,600 field staff in partner organizations

~ 400 NIST staff serving on 1,000 national and international standards committees



© Geoffrey Wheeler

©Robert Rathe

Major Programs

NIST Laboratories

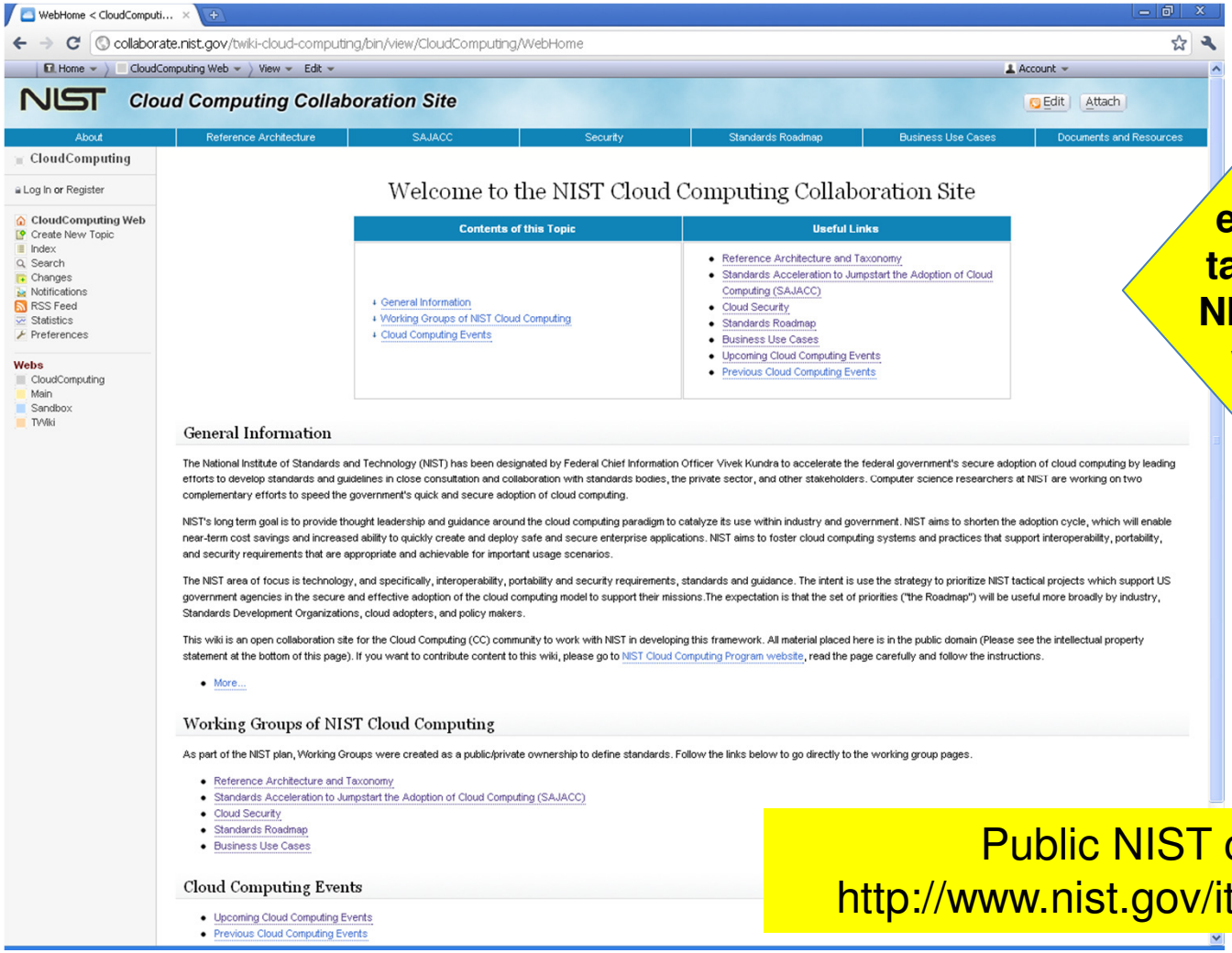
Baldridge National Quality Program

Manufacturing Extension Partnership

National Voluntary Laboratory Accreditation Program (NVLAP)

NIST Cloud Computing Collaboration Site

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome



each strategic & tactical effort is a NIST-led project & working group

Public NIST cloud web site url
http://www.nist.gov/itl/cloud/index.cfm

Information Technology Laboratory Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

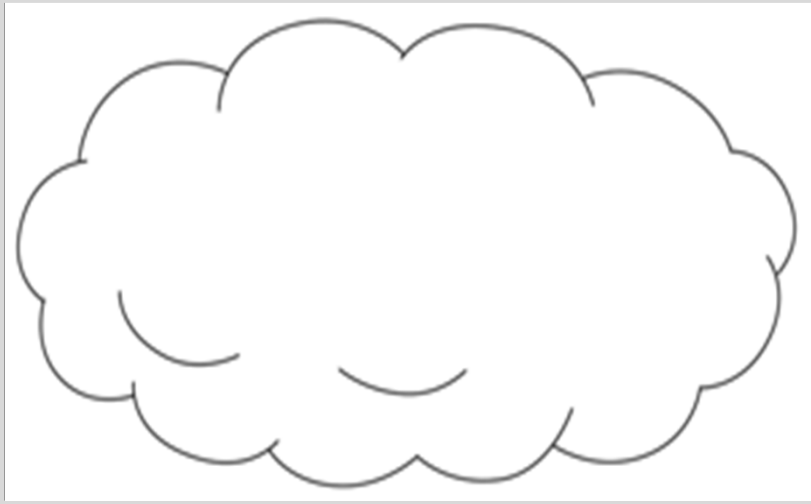
NIST Cloud Computing Reference Architecture
Actors and their Roles

Cloud Consumer
Person or organization that maintains a business relationship with, and uses service from *Cloud Providers*.

Cloud Auditor
A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

Cloud Provider

Person, organization or entity responsible for making a service available to *Cloud Consumers.*



Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers.*

Cloud Carrier
The intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Cloud Provider

- ***Cloud Provider*:** Person, organization or entity responsible for making a service available to *Cloud Consumers.*
- Cloud providers perform different tasks for different service models.

Provider Type	Major Activities
SaaS	Installs, manages, maintains and supports the software application on a cloud infrastructure.
PaaS	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment and administration tools to platform consumers.
IaaS	Provisions and manages the physical processing, storage, networking and the hosting environment and cloud infrastructure for IaaS consumers.

- The activities of cloud providers are discussed in greater detail from the perspectives of *Service Deployment, Service Orchestration, Cloud Service Management , Security* and *Privacy*.

Cloud Carrier

Cloud Carrier: The intermediary that provides connectivity and transport of cloud services between *Cloud Providers* and *Cloud Consumers*.

- Provide access to cloud consumers through network, telecommunication and other access devices.
  - Example: Network access devices include computers, laptops, mobile phones, mobile internet devices (MIDs), etc.
- Distribution can be provided by network and telecomm carriers or a transport agent.
  - ***Transport agent:*** A business organization that provides physical transport of storage media such as high-capacity hard drives.
- A cloud provider shall set up SLAs with a cloud carrier to provide a consistent level of service. In general, the cloud carrier may be required to provide dedicated and encrypted connections.

Cloud Broker

Cloud Broker: An entity that manages the use, performance and delivery of cloud services and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.

The major services provided by a cloud broker include:

- ***Service Intermediation***: A cloud broker enhances a given service by improving some specific capability and provides the value-added service to cloud consumers.
- ***Service Aggregation***: A cloud broker combines and integrates multiple services into one or more new services. The broker will provide data integration and ensure the secure data movement between cloud consumer and multiple cloud providers.
- ***Service Arbitrage***: Service arbitrage is similar to service aggregation, with the difference in that the services being aggregated aren't fixed. Service arbitrage allows flexible and opportunistic choices for the broker. For example, the cloud broker can use a credit-scoring service and select the best score from multiple scoring agencies.

Cloud Auditor

Cloud Auditor: A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

- A cloud auditor can evaluate the services provided by a cloud provider in terms of *security controls*, *privacy impact*, *performance*, etc.
  - For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Auditing is especially important for federal agencies and "agencies should include a contractual clause enabling third parties to assess security controls of cloud providers" (*Federal Cloud Computing Strategy, Feb. 2011*.).

Taxonomies

The science of categorization, or classification, of things based on a predetermined system. (Webopedia)

Main Attributes:

- Typically a controlled vocabulary with a hierarchical tree-like structure
- Terms in a taxonomy have relationships with other terms
- Usually in the form of a parent (broader) / child (narrower)

Benefits:

- Encompasses and labels all significant concepts within a given domain
- Allows users to understand the context of each label

Taxonomy Cloud Terms and Definitions

Level 1:

- **Cloud Service Provider** – Person, organization or higher-level system responsible for making a *service* available to *service consumers*.

Level 2:

- **Cloud Service Management** – Cloud Service Management includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers.

Level 3:

- **Public Cloud** - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. [NIST Definition of Cloud Computing]

Level 4:

- **Data Portability** – The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. [Federal Standard 1037C]