

Cloud Computing - A NIST Perspective and Beyond

Robert Bohn, PhD
*Advanced Network
Technologies Division*

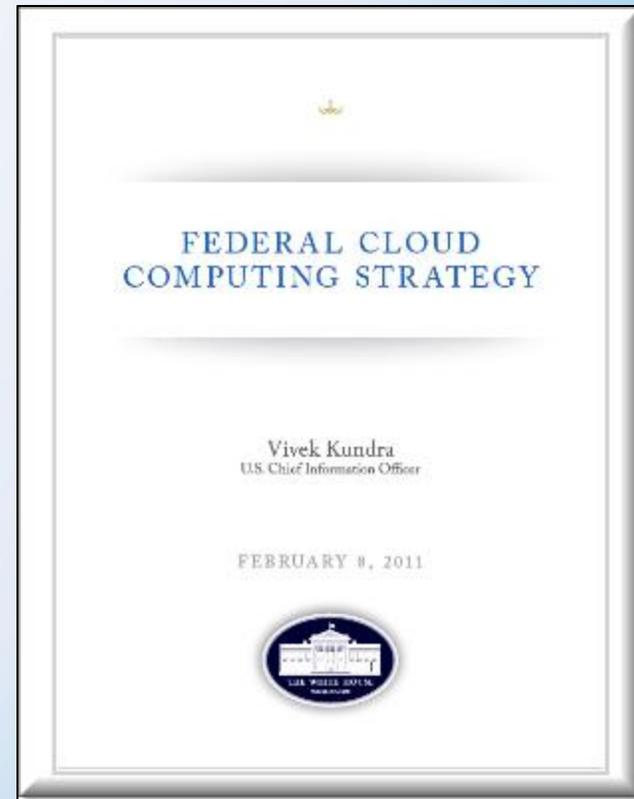
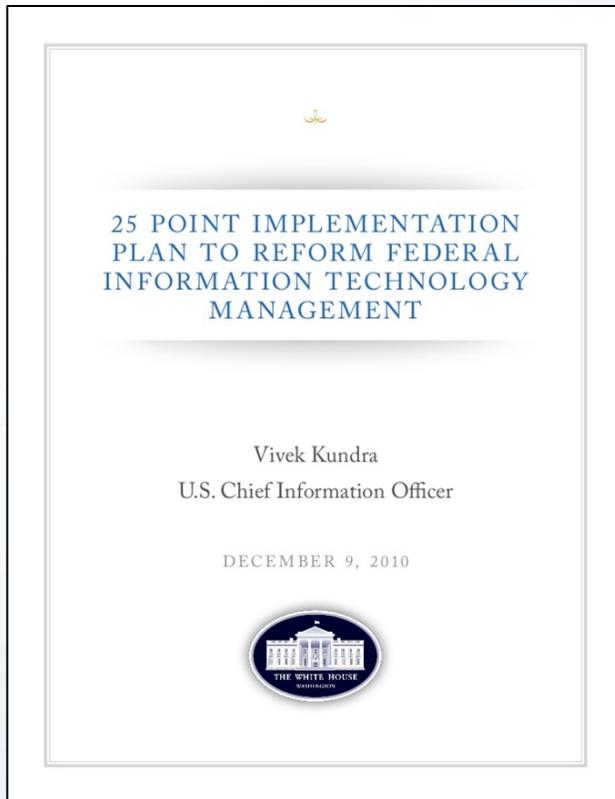
*2014 NASA Goddard IS&T
Colloquia Lecture Series
November 5, 2014*



Cloud Program Overview

- Launch & Objectives
- Roadmap & Requirements
- Future Outlook
- Cloud Computing Standards
- Workshops

Federal IT Strategies

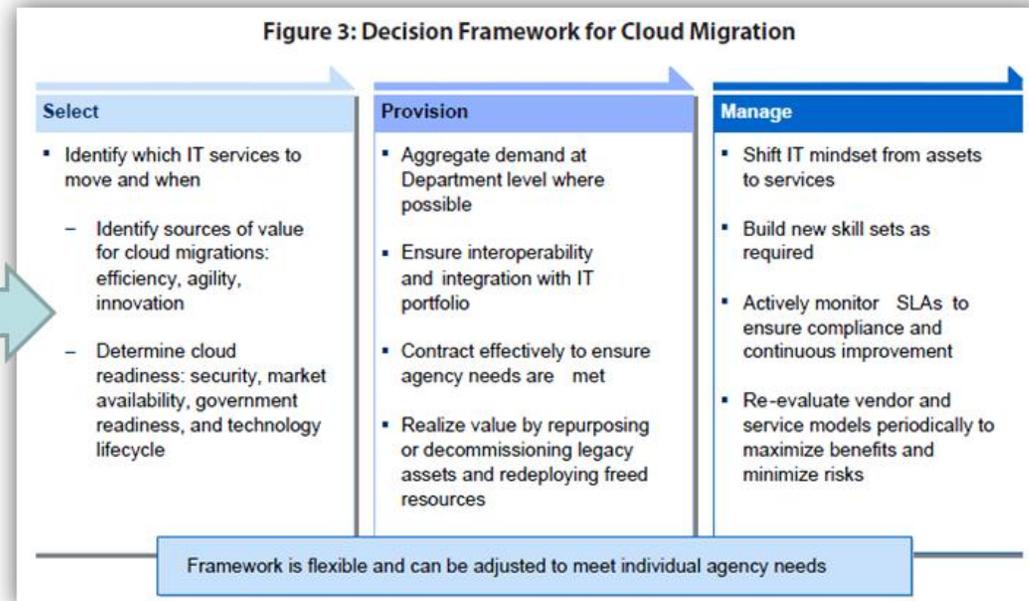
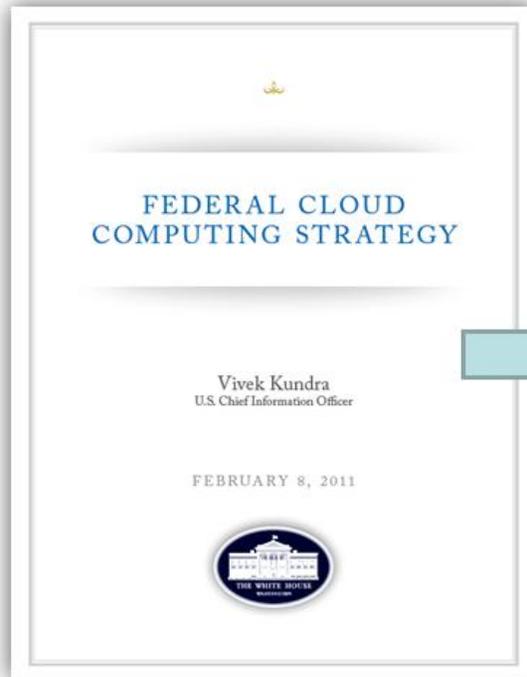


Federal Cloud Computing Strategy

- US IT Budget ~ \$80B/year: Savings ~25%
- Move to cloud when possible.
- Investigate Cloud-applicability for new services
- 3 Agencies -
 - NIST – Standards
 - GSA – Procurement (*FedRAMP*)
 - DHS – Operational Security



Select - Provision - Manage



- **Decisions in Moving to the cloud**
- **Decisions in Provisioning cloud services effectively**
- **Decisions in Managing services rather than assets**

The NIST Cloud Computing Program Goal

To 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 Definition of Cloud Computing

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

3 Service Models

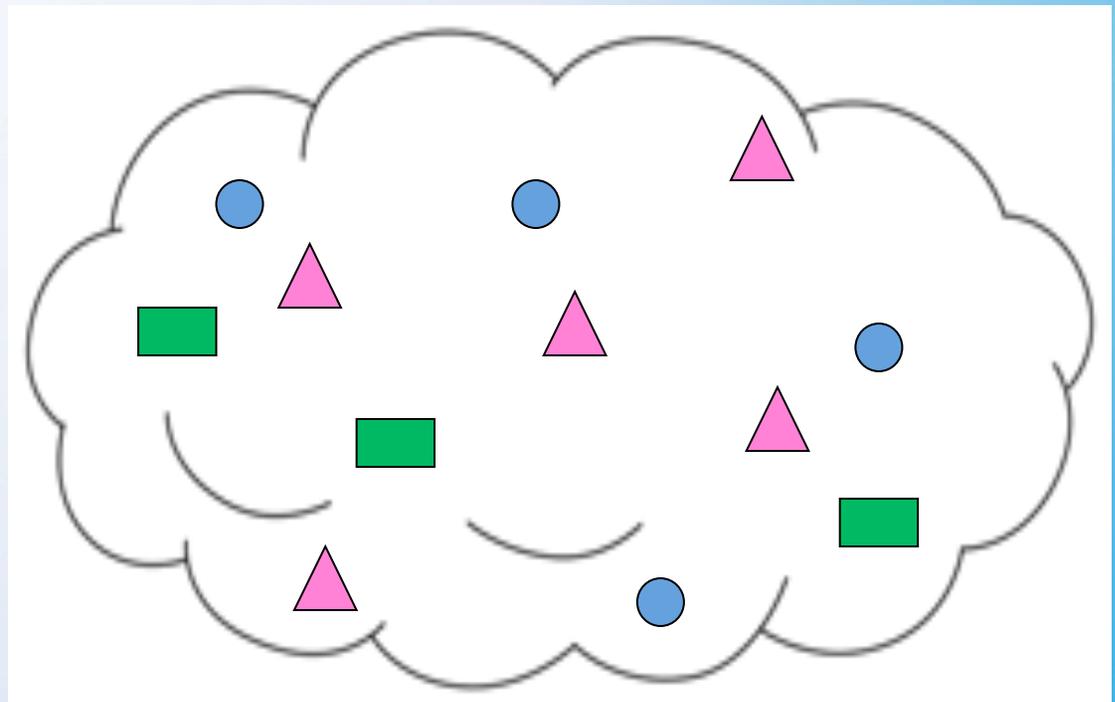
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4 Deployment models

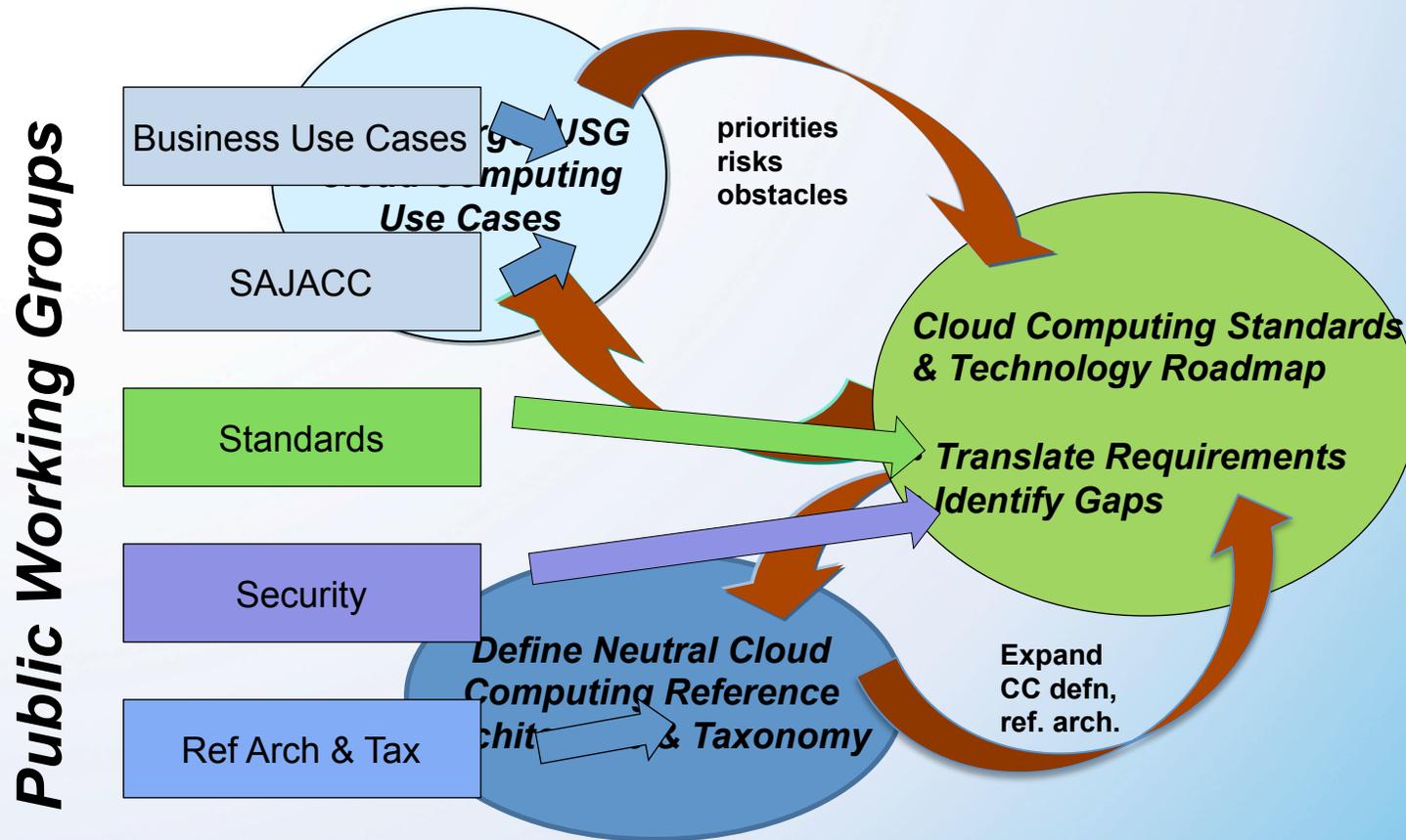
- Public, Private, Community, Hybrid

5 Essential Characteristics

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



How to build a USG Cloud Computing Technology Roadmap



NIST Cloud Computing Reference Architecture

Actors and their Roles

Cloud Consumer

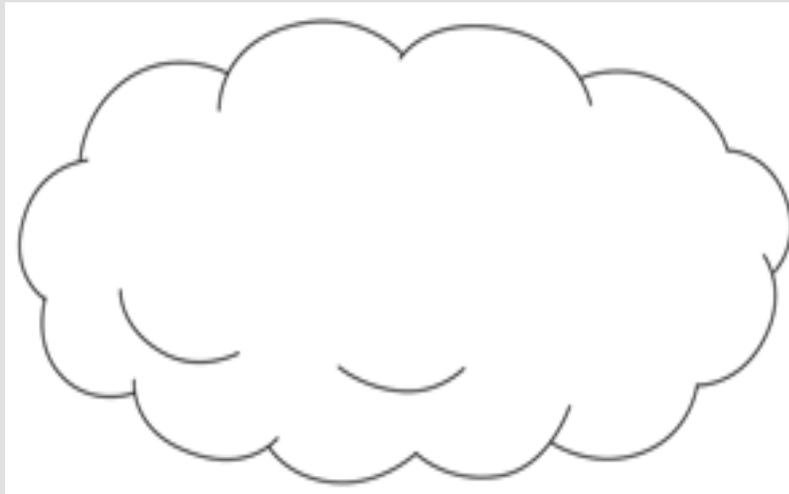
Person or organization that maintains a business relationship with, and uses service from *Cloud Providers*.

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*.



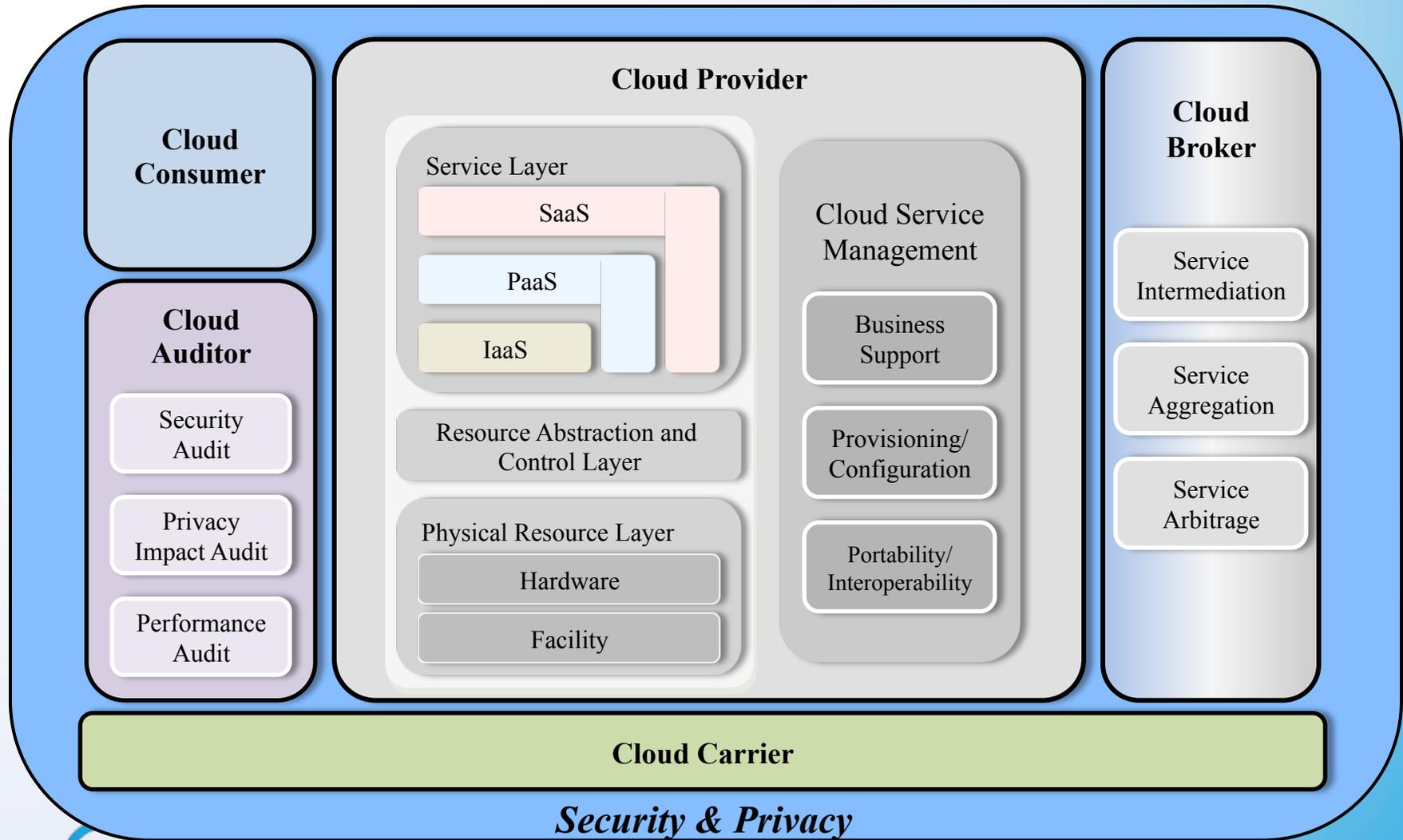
Cloud Broker

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

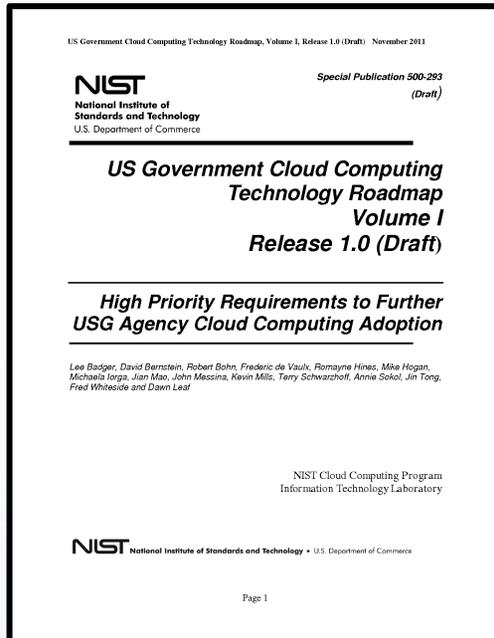
Cloud Carrier

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

NIST Cloud Computing Reference Architecture



USG Cloud Computing Roadmap - Volume I



Core Elements:

- **Prioritized strategic and tactical requirements that must be met for USG agencies to further cloud adoption;**
- **Interoperability, portability, and security standards, guidelines, and technology needed to satisfy these requirements;**
- **Recommended list of Priority Action Plans (PAPs) -- candidates for voluntary self-tasking by the stakeholder community.**

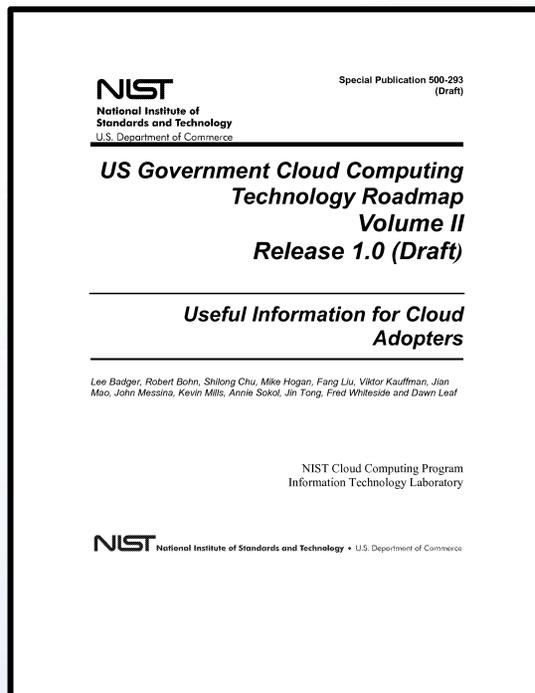
Collaboration through public working groups & Federal Cloud Computing Standards & Technology Working Group

Intent is to leverage PAPs that are identified as complete or under way by cloud stakeholder community; some may fall within NIST scope



USG Cloud Computing Roadmap - Volume II

Use collaboration through public working groups & Federal Cloud Computing Standards & Technology Working Group to continue to validate findings



Reference Architecture & Taxonomy

- Recommend Industry Mapping so that USG agencies & others can more easily and consistently compare cloud services
- In parallel, support formal standards development process leveraging the reference architecture

Standards

- Provide avenue for USG agency engagement
- Continue standards roadmap

Target Business Use Cases & SAJACC

- Expand initial use case set & use SAJACC to identify gaps

Security

- leverage working groups to finalize special publication focusing on challenging security requirements
- Continue technical advisor role – e.g. FedRAMP, continuous monitoring, conformity assessment system



USG Cloud Computing Technology Roadmap Requirements (500-293)

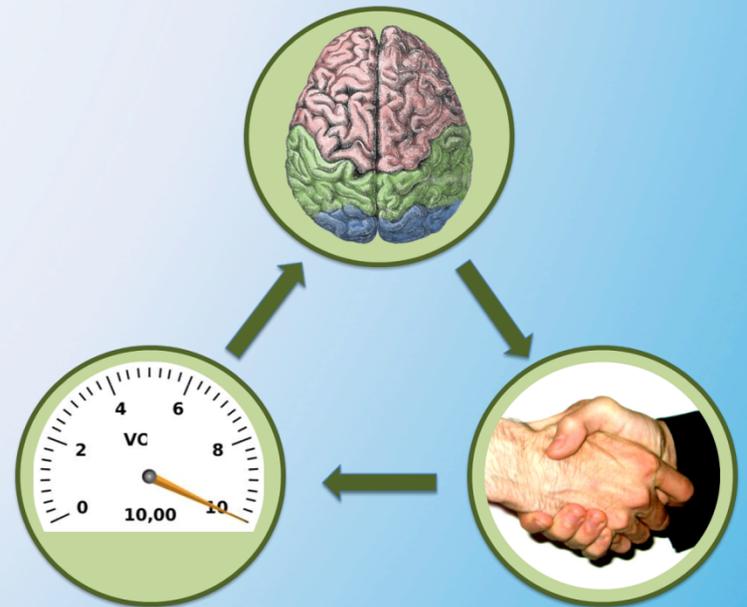
1. International voluntary consensus-based standards
2. Solutions for High-priority Security Requirements, technically decoupled from organizational policy decisions
3. Technical specifications to enable development of consistent, high-quality Service-Level Agreements
4. Clearly and consistently categorized cloud services
5. Frameworks to support seamless implementation of federated community cloud environments
6. Updated Organization Policy that reflects the Cloud Computing Business and Technology model
7. Defined unique government regulatory requirements and solutions
8. Collaborative parallel strategic “future cloud” development initiatives
9. Defined and implemented reliability design goals
10. Defined and implemented cloud service metrics

Three parts to the process

Decide - lay out the requirements for the service

Agree - the **MSA/SLA** is the agreement connecting customer and provider

Measure - are the SLA objectives met ?



Cloud Service Level Agreements (SLAs)

- **Cloud Service Level Agreement:** A document stating the technical performance promises made by the cloud provider, how disputes are to be discovered and handled, and any remedies for performance failures. (NIST SP 800-146). *Differs from Master Service Agreement (MSA)*
- No standard cloud computing contracts exist.
- Little agreement with respect to:
 - which elements should appear within a SLA
 - which metrics to use
 - how terms are defined
- Industry and USG need to develop and adopt consistent technical specifications, of high quality and completeness, to enable the creation and practical evaluation of Service-Level Agreements (SLAs) between customers and cloud providers.

Contents of SLA

Business Level Objectives

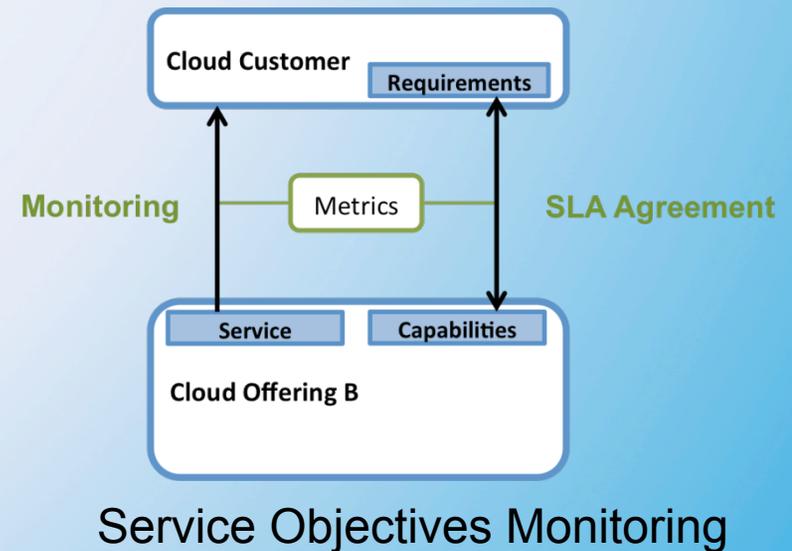
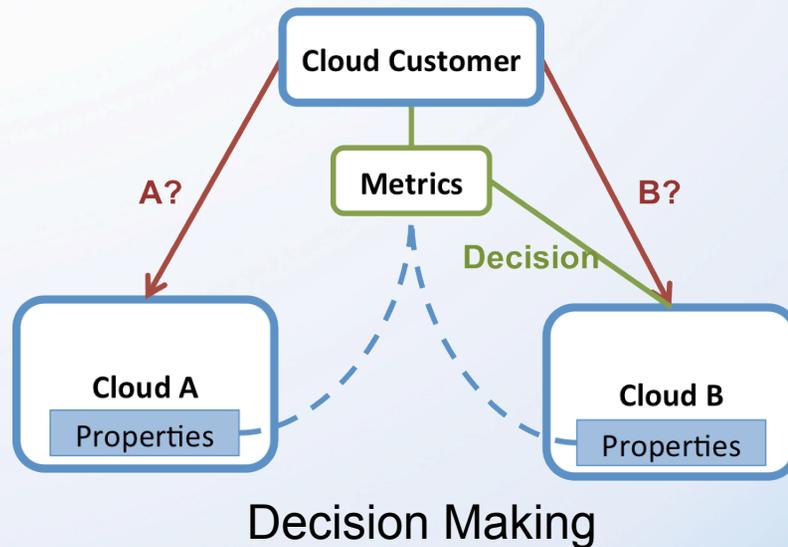
- Roles & Responsibilities
- Requirements
- Operational Policies
- Continuity
- Limitations
- Financial
- Glossary of Terms

Service Level Objectives

- Resources
- Performance Indicators
- Service Deployment
- Service Management
- Description
- Security
- Privacy

Service Level Agreements (SLAs) - Metrics

- Metrics for Selecting Cloud Services
- Metrics in Service Agreements (SAs)
- Metrics in Monitoring



SLA Performance Metric - *Service Availability*

- An Availability Metric could be based on different definitions for *measures*:
- Most commonly, availability is evaluated based on the percentage of “uptime” (available state) of a resource, over some period of time.
- **service_uptime_percentage**: the percentage of qualified service availability time over the observation time, as defined by the *expression*:

$$\textit{service uptime} \% = \text{qualified_uptime_total} / \text{observation_time_total} * 100$$

Future Outlook

The convenience of *reliable*, *trusted* and *measurable* cloud services become a foundational element of the global economy.

These services, constructed with open standards and metric based building blocks, form the basis for a collection of interconnected clouds to:

- drive innovation
- facilitate world-wide collaboration & shared knowledge
- provide positive environmental and economic impacts

Federated Cloud

- Develop a common understanding and definition of what a Federated Cloud entails
- Identifying the requirements needed to reach the achieve a Federated cloud,
- Identify the technology and standards gaps that need to be addressed in order to enable the Federated Cloud
- Provide a path to achieving the Federated Cloud



Pooling of resources from disparate, potentially heterogeneous, cloud systems where interoperability and portability enable sharing, migration, and redundancy which is all ensured through a common mechanism (such as central management system or a common API), and where identity and authorization management mechanisms are established.

Cloud Services

- Explore the essential characteristics of cloud services and examine the intricacies that exist between cloud service types.
- Customers will make better selections of cloud services
- Customers will be able to objectively evaluate, compare, and select between products from cloud vendors, and
- Cloud Providers will have clear guidance where interoperability and portability must exist within similar categories of cloud services

Interoperability & Portability

- Types of cloud computing interoperability and portability - relationship and interactions
- Contexts where interoperability and portability are relevant in cloud computing, with respect to the cloud computing reference architecture; and
- Common terminology and concepts used to describe interoperability and portability.



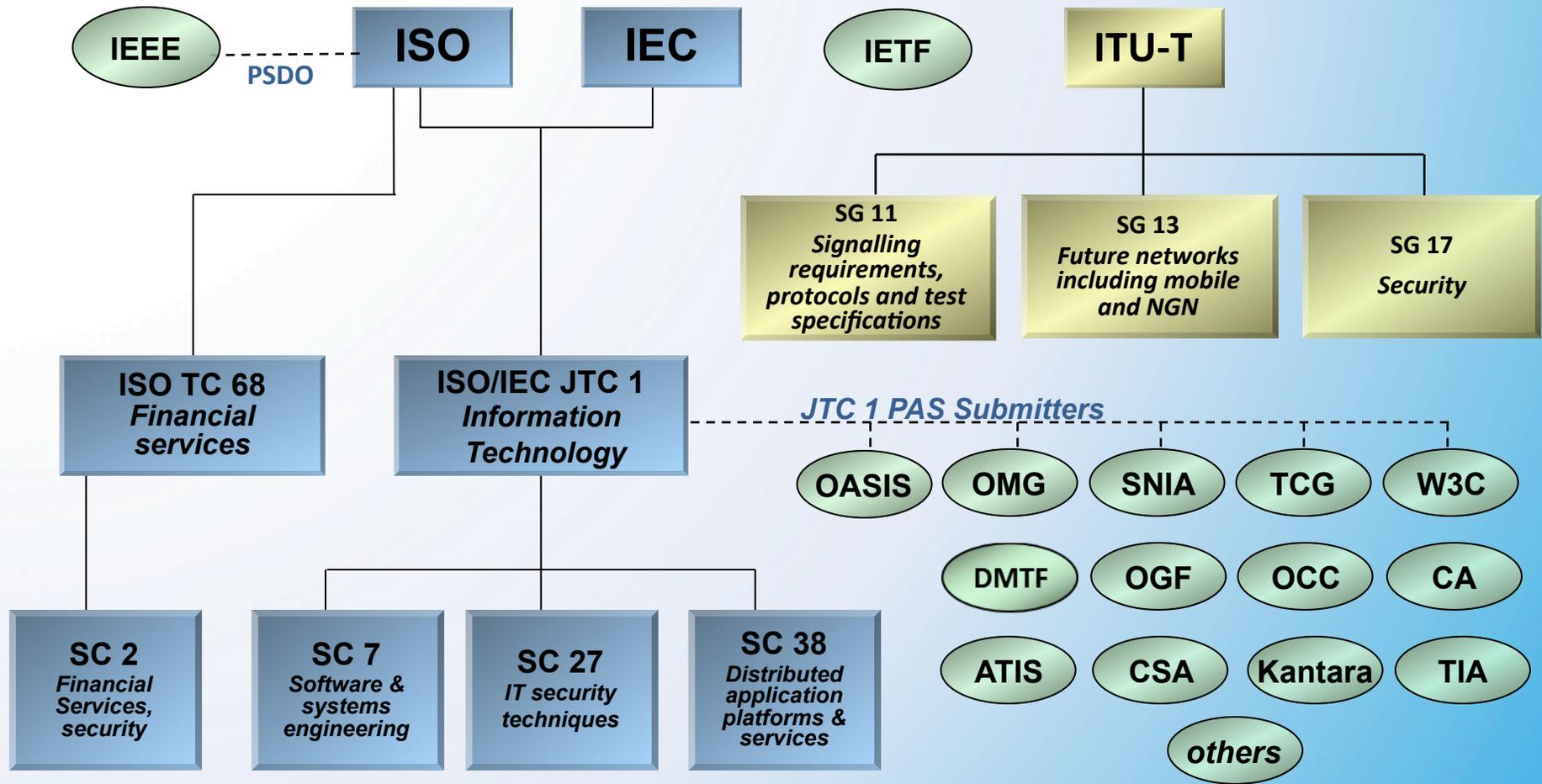
<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudInteroperability>

Status and Next Steps

- Developed
 - Reference Architecture & Taxonomy
 - Security Reference Architecture
 - Descriptions of Cloud Broker
 - Standards Inventory
- Developing Cloud Actor descriptions
 - Cloud Consumer
 - Cloud Carrier
 - Cloud Auditor
- Developing a Cloud Service Metric Model
- PWG's in Cloud & Accessibility, Federated Cloud
- Key Management for Cloud

Standards Activities

Cloud Computing Standards Developers



Key: PSDO = Partner Standards Development Organization; PAS = Publicly Available Specification;

- = private sector, national member-based international standards body;
- = UN agency, member state-based international standards body;
- = international consortium standards developer

Cloud Standards: *Participation in National and International Arenas*

- CT with ISO/IEC/JTC 1 SC38 WG3 RA&Tax 17788/17789
 - Annie Sokol, Editor Collaborative Team w ITU-T
 - Final Intl Standard (8/2014)
- SC38 WG3 19086 SLA Framework & Terminology
 - Eric Simmon, Editor
 - Committee Draft – Fall 2014 Part 1-Framework; Part 2-Metrics; Part 3 - requirements
- SC38 Study Group on Future Work
 - John Messina, Convener
 - Annie Sokol – Interoperability Lead: New Work Item Accepted (9/2014)
- IEEE SG P2301– Guide for Cloud Portability and Interoperability Profiles (CPIP)
- IEEE SG P2302 - Standards for Intercloud Interoperability and Federation (SIIF)

NIST Cloud Computing Forum & Workshop Series

- 7 events to date
- Initiated May 2010
- Purpose
 - Communication
 - Outreach
 - Building relationships
 - Forming communities
- Special Events
 - Cloud & Big Data – January 2013
 - Cloud & Mobility – March 2014



NIST Cloud Computing Forum & Workshop Series

The Intersection of Cloud and Mobility

March 25-27, 2014

Gaithersburg, MD

Keynote Speakers –

Pamela Wise-Martinez – Office of the Director of National Intelligence

Jacob West – CTO, Hewlett-Packard

Chris Kemp, Nebula

Teri M. Takai, CIO- US Department of Defense

Mario Gerla, UCLA



NIST Cloud Computing Special Publications

- CC Standards Roadmap500-291
- CC Reference Architecture500-292
- USG CC Technology Roadmap500-293
- *Security Reference Architecture.....500-299*

- Guidelines on Security and Privacy800-144
- Definition of Cloud Computing800-145
- CC Synopsis & Recommendations.....800-146

Searchable as “NIST SP xxx-yyy”



Contacts

Dr. Abdella Battou	abdella.battou@nist.gov	CC Lead/ANTD Chief
Dr. Robert Bohn	robert.bohn@nist.gov	Program Mgr
John Messina	john.messina@nist.gov	RA/Tax Co-Convener
Dr. Michaela Iorga	micheala.iorga@nist.gov	Security
Annie Sokol	annie.sokol@nist.gov	Standards
Mike Hogan	michael.hogan@nist.gov	Standards
Eric Simmon	eric.simmon@nist.gov	SLA/Standards
Frederic de Vaultx	frederic.devaultx@nist.gov	Metrics
Lisa Carnahan	lisa.carnahan@nist.gov	Conformity Assessment

NIST ITL Cloud Computing Home Page

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

NIST Cloud Computing Collaboration Site (twiki)

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

