NIST Strategy to build a USG Cloud Computing Technology Roadmap

The **National Institute of Standards and Technology (NIST) has been has been asked by the United States Chief Information Officer to assume a technology leadership role**[1] in support of United States Government (USG) secure and effective adoption of the Cloud Computing[2] model to reduce costs and improve services. The working document describes the NIST Cloud Computing program efforts in this context.

1.0 EXECUTIVE SUMMARY

Cloud computing offers the promise of cost savings and increased IT agility. The paradigm of cloud computing evolved as underlying technologies have sufficiently matured to enable more efficient IT models to leverage resources. The paradigm emerged as a result of the ability to use pooled IT resources, and the convergence of IT trends that enable more effective data center utilization, including: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.

However, cloud computing technology also upends traditional approaches to datacenter and enterprise application design and management. While cloud computing is being used, security, interoperability, and portability are cited as barriers to broader adoption.

NIST plays a central role in defining and advancing standards, & collaborating with USG Agency CIOs, private sector experts, and international bodies to identify and reach consensus on cloud computing technology & standardization priorities. Through its strategic efforts to collaboratively develop a USG Cloud Computing Technology Roadmap, NIST is helping to translate mission requirements into technical portability, interoperability, reliability, maintainability and security requirements. The roadmap document is the mechanism being developed by the NIST Cloud Computing program to define and communicate these prioritized requirements. Focusing its efforts using these priorities, NIST is working with other stakeholders to develop the standards, guidance, and technology which must be in place to enable the secure and effective deployment of the cloud computing model.

NIST is targeting issue of the first draft of the NIST USG Cloud Computing Technology Roadmap as an Interagency Report (IR) at the end of FY2011

[1] Ref http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

[2] NIST Special Publication 800-145 (Draft), The NIST Definition of Cloud Computing (Draft), *Recommendations of the National Institute of Standards and Technology,* Peter Mell, Timothy Grance

That USG Cloud Computing Technology Roadmap will include work completed by the NIST Cloud Computing strategic and tactical projects, the US Federal CIO Council Cloud Computing Advisory Council Standards Working Group, and NIST chaired public working groups. The latter are designed to integrate NIST internal efforts with broader collaborative and external cloud computing activities. The NIST chaired cloud computing public working groups include: 1) Target USG Business Use Cases, 2) Neutral Reference Architecture & Taxonomy, 3) Standards Roadmap, 4) Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC), and 5) Cloud Security.

These projects and working groups, integrated and working in parallel and iteratively, are developing interim products which are a subset of the broader NIST USG Cloud Computing Technology Roadmap scope.

Similarly, the NIST USG Cloud Computing Technology Roadmap is one of several complementary and parallel United States (US) government Cloud Computing initiatives defined in the broader Federal Cloud Computing Strategy issued in February 2011. USG agencies are developing agency specific Cloud Computing implementation strategies using a common decision framework to determine how the cloud computing model will be deployed to support mission IT requirements. The General Services Administration (GSA) and Department of Homeland Security (DHS) also have key roles in the overall US Federal Cloud Computing Strategy.

Through its efforts, NIST aims to provide thought leadership and guidance around the cloud computing paradigm to catalyze its use within industry and government. NIST aims to shorten the adoption cycle, which will enable near-term cost savings and improved ability to quickly create and deploy enterprise applications.

Updated information on the NIST Cloud Computing Program strategic and tactical projects is available through the NIST Information Technology Laboratory Cloud Computing web site[3].

Public stakeholder participation is encouraged. All parties are invited to directly participate in the collaborative voluntary efforts, register as public working group members, and to directly contribute through the NIST ITL Cloud Computing collaboration website[4].

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

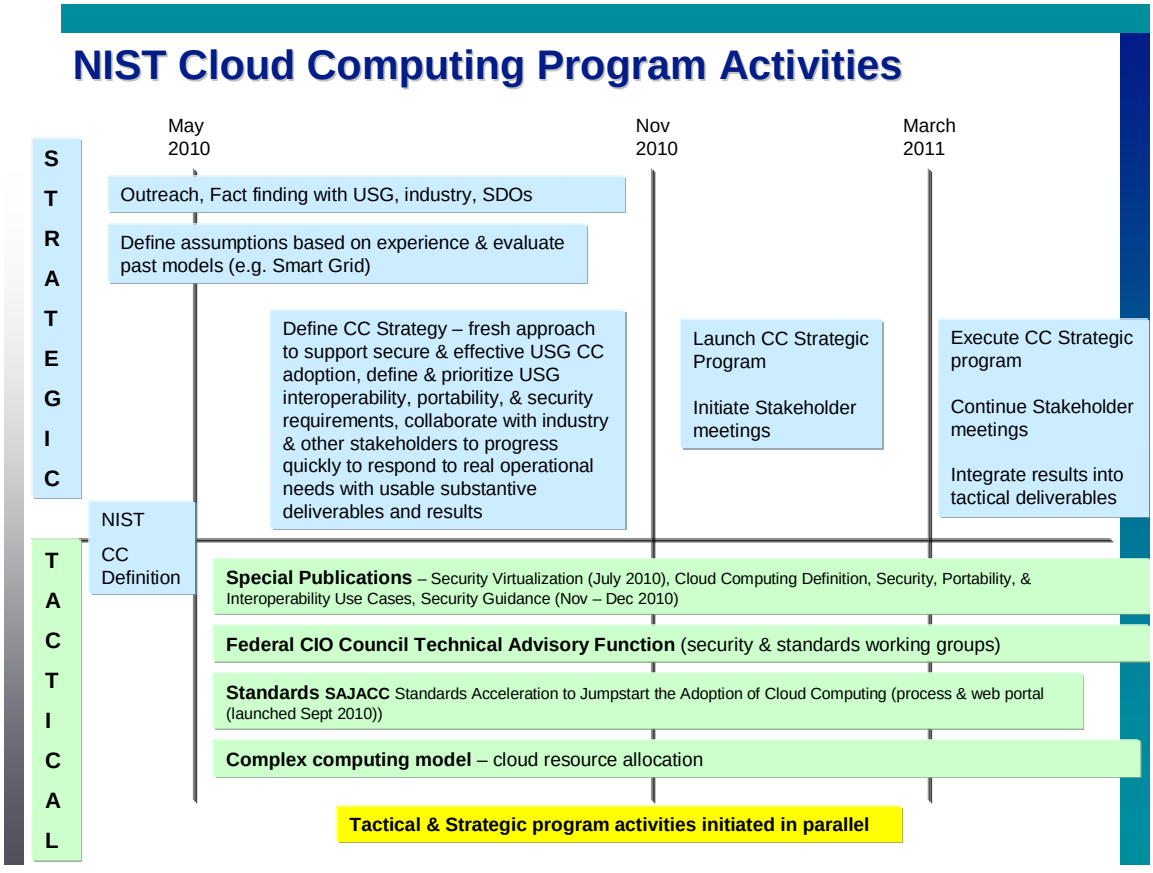
[4] http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome

2.0 NIST Cloud Computing Program and Strategy Evolution

Background

The NIST approach to advancing cloud computing technology and innovation, to further United States government adoption, has been shaped by the rapid development of the cloud computing paradigm and services. The pace of cloud computing technology rendered a sequential top-down strategic and tactical projects' plan approach not timely enough. In recognition of the industry and technology dynamics, NIST took the tact of defining its strategic plan and objectives in parallel with initiating tactical efforts.

The NIST Cloud Computing Program Strategic and Tactical efforts are integrated as shown below:



Prior to May 2010, NIST focused on basic tactical activities that are fundamental to any emerging IT technology. The most visible were public dissemination of the NIST Cloud Computing Definition and level of effort support

in the role of technical advisor to the Federal Chief Information Officers' (CIO) Council. These efforts were focused on the need for federal "guidance" related to effective adoption of cloud computing. Clear high priorities were leading and facilitating the development of Cloud Computing standards, particularly to address security, interoperability, portability and address the risk of "vendor lock-in" to a particular cloud service provider solution.

A set of ***key tactical activities*** have proven to be effective in the development of any emerging technology model. These include, but are not limited to:

- developing technical and security guidance starting with a foundation of an existing knowledge base and incrementally and iteratively refining the guidance as a technology evolves,
- applying use case methodology to define and refine interoperability, portability and security requirements, and executing test plans against these requirements to assess the extent that interface specifications satisfy these requirements, and
- simulating complex computing models.

NIST initiated projects to begin work on these fundamental tactical information technology objectives in May of 2010, has continued these efforts, produced deliverables from these efforts, and continues to work these efforts.

However, at the same time, NIST recognized a need to form a strategy based on an understanding of the highest priority mission oriented requirements and issues which must be addressed to apply cloud computing technology, in order to focus the NIST tactical efforts and ensure that they best use scarce resources and address the most important requirements (from an adopter and industry provider as well as NIST computer scientist and researcher perspective.)

In this context, under the guidance of the United States Chief Information Officer and Director[5] of the National Institute of Standards and Technology, NIST has developed an informed and considered ***strategy to focus on interoperability, portability and security requirements*** which must be met to support United States government agencies in the safe and effective application of the cloud computing model to support their missions.

In May 2010, NIST expanded its public outreach program to host a public Cloud Computing Forum and Workshop**. The purpose was to initiate broader dialogue with academia, Standards Development Organizations, industry and government stakeholders, and to publically launch a federal government initiative focused on interoperability, portability, and security**

[5] N.b. Then Director of the National Institute of Standards and Technology was confirmed as the Under Secretary of Science and Technology in 2011.

standards. This included the Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC) strategy, process and portal. The forum discussed the Federal Risk and Authorization Management Program (FedRAMP), and NIST role as technical advisor to the Federal CIO Council Cloud Computing Advisory Council (CCAC). NIST briefed the development of Special Publications related to Cloud Computing. The event marked an increased volume and level of outreach activity. **In July 2010**, these same priorities where presented in Congressional Testimony by the NIST ITL Director, and recommended by a General Accounting Office (GAO) report issued in the same timeframe.

NIST Strategic Cloud Computing Approach – How the NIST Strategy was Developed

Throughout the mid 2010 timeframe, the Federal CIO and NIST executive management assessed the NIST Cloud Computing program scope and effectiveness. The NIST tactical efforts were deemed to be effective in support of the general advancement of Cloud Computing technology and standards adoption, but not broad enough in scope or sufficiently targeted to bring together the USG OCIO, SDO, and industry stakeholders to focus on specific US government Cloud Computing requirements in order to "get ahead of the Cloud" technology trend.

This assessment and the resulting NIST Cloud Computing Strategy which was defined in the fall of 2010 (consistent with and part of the overall US government Cloud Computing strategy) was primarily based on three factors:

- the opinions and requirements expressed by federal, state, and local governments,
- the opinions and information provided by standards development organizations, industry and other IT community stakeholders, and
- lessons learned through initiatives such as the Smart Grid Strategy and Roadmap program.

What NIST Learned

After its first Cloud Computing Forum and Workshop in May 2010 NIST sought and considered the opinions and requirements expressed by the stakeholders described above.

Federal CIOS need and want answers to practical operational questions – how does an agency protect its data if it doesn't physically control the hardware and software used to store, transport and process the data? Is this an option – or is the current approach, building a private cloud where control is maintained by the agency the only answer? What are the rules? How does the agency decide?

Industry is confident in its technical depth, and the ability to solve technical problems if requirements and policy are defined. Yet, there is an interesting parallel that surfaces when major cloud computing service providers are asked the question, "How does an agency know its data is secure in the provider's environment?" In practice, the provider often answers that (the provider's organization) controls the data center and the security infrastructure and offers to share information about its security measures with potential consumers. In other words, industry providers often answer the question the same way that government agencies answer – retention of physical control.

Clearly there is a need to define the risks associated with different cloud computing delivery models (private, public, community and hybrid) and service models (software, platform, and infrastructure), and to provide guidance for and make risk based decisions. This is needed to move past the tendency to polarize cloud adoption at two ends of the spectrum – public cloud for systems and data with lower security requirements and private cloud for data where the consequences of a security incident are deemed unacceptable.

In a perfect world there would be sufficient information to analyze and write a prescriptive "rule book" for cloud computing that agencies could read to remove all uncertainty in decision making BEFORE the cloud computing is deployed.

However, the nature of an emerging technology, including the emerging cloud computing model, is such that there is an insufficient installed base and therefore information at present to do this. There are at least two drivers that drive the uncertainty. One is the nature of innovation – innovation occurs in response to the need to solve operational problems that emerge over time. In other words, the full extent of the innovation that will occur in cloud computing is not known at present – some set of the technology doesn't exist yet. A second driver is the relationship between the installed base of a technology model and the knowledge base. Some information only surfaces through application and experience. The current installed base of the cloud computing model is relatively small as compared to the entire spectrum of computing services. Most experience relates to infrastructure services, the most mature outsourced service model.

These factors do not invalidate the need of US agencies for specific guidance; the factors affect the circumstances under which effective guidance can feasibly be developed (compared to the case of a mature technology model.) Bottom line, we need to develop guidance given the reality of the constraints that an emerging technology model creates.

NIST listened carefully to industry consortia, academia, standards development organizations (SDOs), and international, state and local government agencies.

Industry, SDOs, and government entities endorse the need for a neutral reference architecture for cloud computing that can be used as a frame of

reference for discussion. A performance based reference architecture that is more detailed than the broadly used NIST Definition of Cloud Computing is needed to help the federal CIO community understand and categorize various cloud offerings. The reference architecture needs to be abstract to a high enough level to avoid specifying a specific vendor solution reference implementation to ensure that innovation is not constrained, and to ensure a level playing field for all stakeholders – vendors, nation states, and standards bodies. The goal is to help illustrate and understand the complexities of cloud computing services and offerings – specifically to help US government agencies compare "apples to apples" in terms of cloud computing services, in consideration of these services to support their missions.

There are advocates of formal consensus based standards development processes and advocates of the market driven defacto standards model. There are valid viewpoints in each. Standards must be completed with due diligence and consensus processes to ensure they are of a quality and completeness such that they will be broadly adopted and do not constrain technology innovation, and are not used as a barrier to foster competitive advantage. Historically there have been cases where the duration and organizational dynamics associated with processes of due diligence and consensus building have rendered the formal standards model ineffective – alternative defacto standards were adopted. The discussion is much more complex than this paragraph implies. The point is that the balance of the pros, cons, and practical realities of standards development need to be weighed in.

In consideration of all of these factors, NIST developed a strategy to hone in on the real and perceived obstacles of cloud computing adoption, translate these into prioritized actionable requirements, and to collaborate closely with industry in order to facilitate the closure of these requirements as quickly as possible.

NIST developed the strategy as described below, and proposed it formally in the November 2010 NIST Cloud Computing and Forum II, hosted by NIST at its Gaithersburg, Maryland facility.

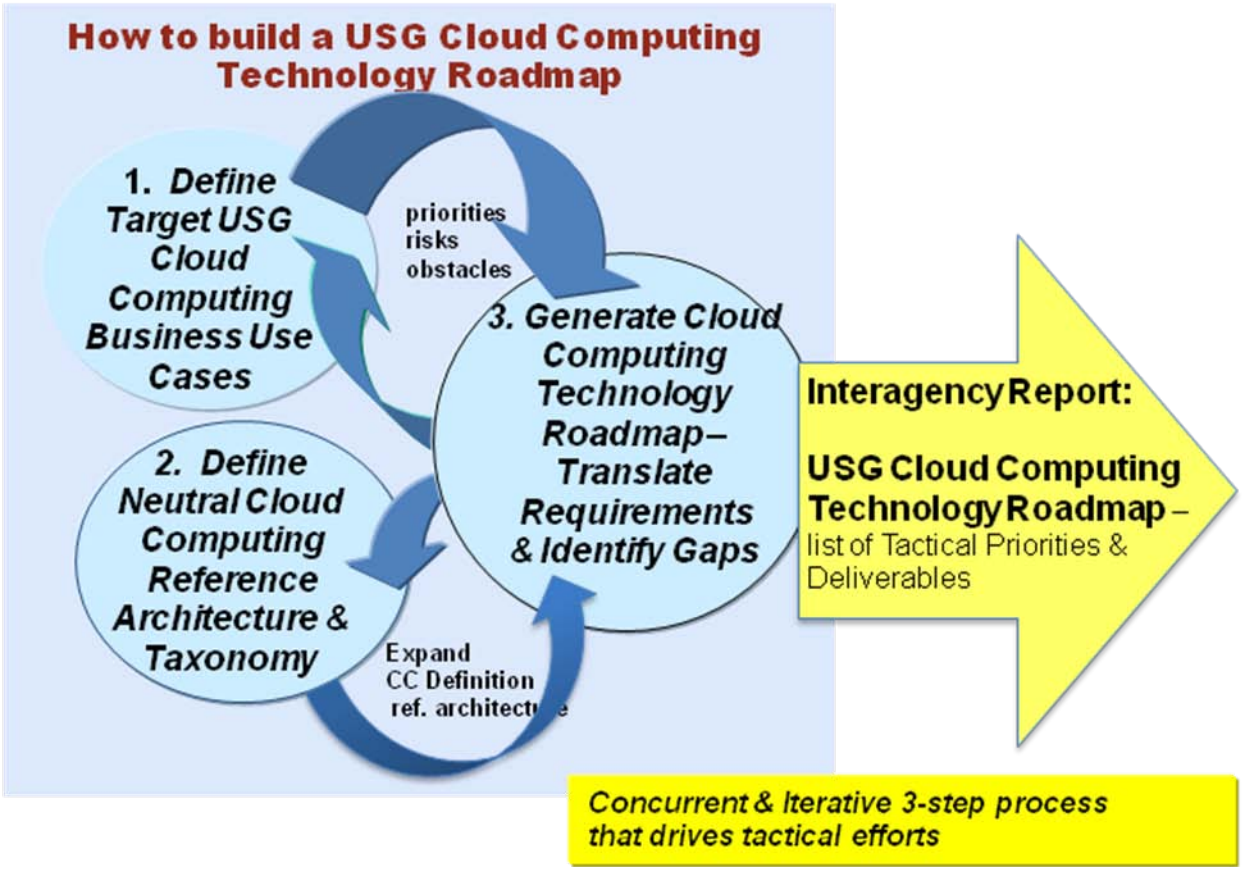
3.0 Overview: NIST Strategy to Build a USG Cloud Computing Technology Roadmap

Goal

The proposed ***Strategy to Build a USG Cloud Computing Technology Roadmap*** is designed to accelerate secure and effective United States government Cloud Computing adoption, define and prioritize USG interoperability, portability, & security requirements, collaborate with stakeholders, and to progress quickly to respond to real operational needs with usable substantive deliverables.

Strategy Definition

The NIST led strategy to collaboratively develop a USG Cloud Computing Technology Roadmap includes three major process steps:



1. Define USG Cloud Computing Target Business Use Cases (set of candidate deployments) for Cloud Computing model options, to "nail down" specific risks, concerns and constraints;

In parallel with Step 1:

2. Define Neutral Cloud Computing Reference Architecture and Taxonomy to extend the NIST cloud computing model with industry & USG experts, and use as frame of reference to facilitate communication; and

iteratively, and incrementally as there is progress from Steps 1 & 2:

3. Generate Cloud Computing Technology Roadmap – Iteratively Translate, Define & Track Cloud Computing Priorities by matching requirements from USG target cloud operational scenarios (Business Use Case examples) to

the reference architecture & taxonomy components that address them in order to identify "gaps" in the standards, guidance, and technology needed to satisfy the requirements.

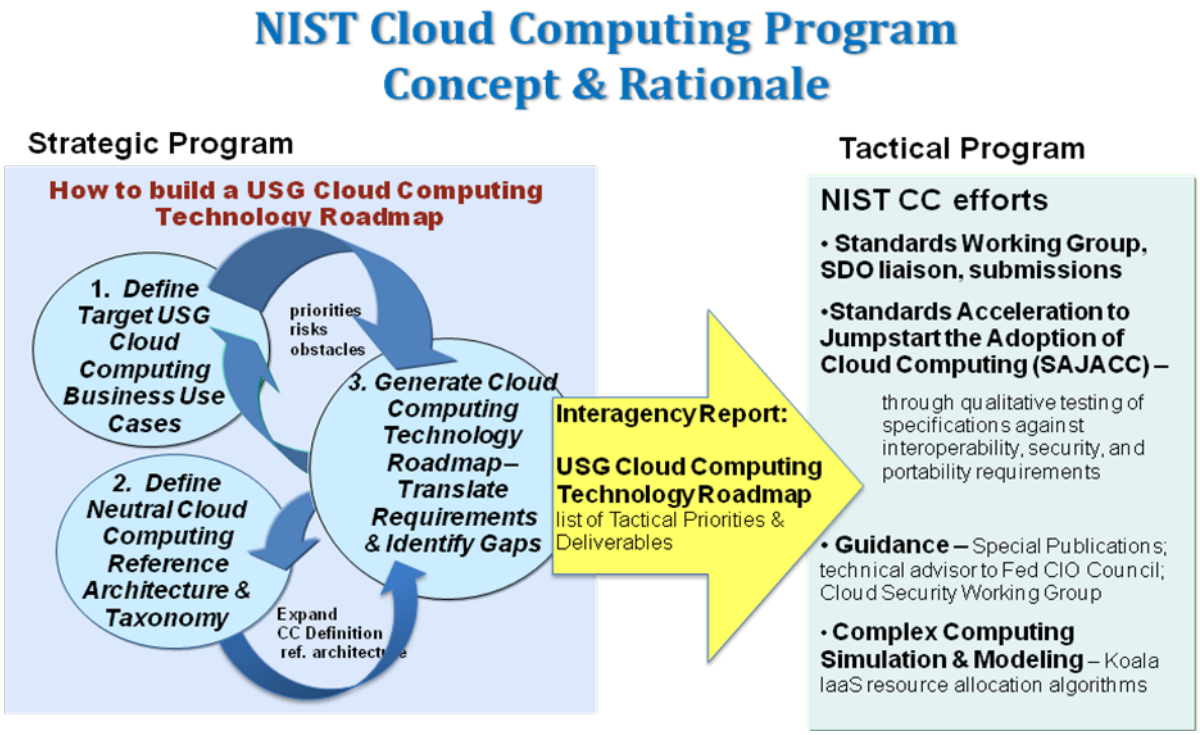
This process is designed to identify technical issues and apply industry expertise to see where they are addressed, identify and hand-off issues to the appropriate tactical organization or process for resolution (needed standard, policy, R&D, prototype or pilot, procurement, governance, cost driver), leverage information for the broad community, and iteratively send scenario alternatives or reference model questions to working groups.

4.0 Strategy in the Context of the NIST Cloud Computing Program

From the NIST perspective, a key element of the approach is the integration of the Strategic and Tactical elements of the NIST Cloud Computing program.

Each Strategic Process represents a project and public working group for NIST. This is the mechanism that we use to ensure that the priorities which are defined in the USG Cloud Computing Technology Roadmap.

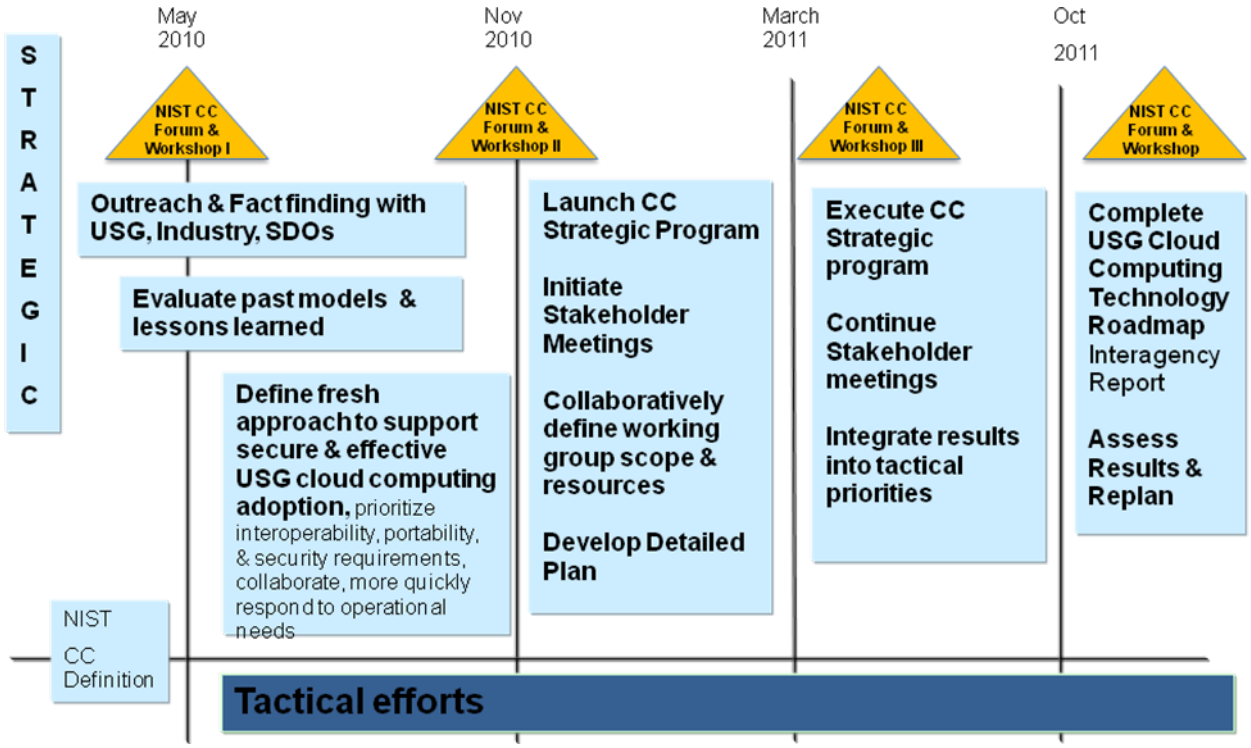
The roadmap, which is a prioritized list of real USG Cloud Computing adoption interoperability, security, and portability (and reliability and maintainability) requirements, then drives the NIST Tactical Cloud Computing efforts.



The Tactical NIST efforts listed above are projects, and in some cases related public working groups.

The NIST strategic cloud computing program efforts are and will continue to be planned and executed in parallel with ongoing tactical efforts. The NIST tactical efforts are effective and necessary – the goal of the strategy is to drive the tactical efforts to make them even more effective – more responsive to US government agencies operational requirements. This approach ensures that NIST is not only doing good work, but working on the "right things" in the sense of reflecting and leveraging the cloud computing stakeholder community perspectives and efforts. (n.b. NIST also integrates its projects with other broad initiatives such as Cyber Security, Smart Grid, Health IT, Voting through the involvement of subject matter experts from these disciplines.)

5.0 Cloud Computing Program Planning and Execution timeline



- As described previously, **May through November 2010**, NIST listened to industry stakeholders and developed the collaborative strategy concept

- In the **November 2010** NIST Cloud Computing Forum and Workshop II, NIST publically presented the concepts of the ***NIST Strategy to Develop a USG Cloud Computing Technology Roadmap***.

- The strategy was received positively by the stakeholder community. In the same event, NIST facilitated a one-day public workshop where a broad set of voluntary partners, representing all of the stakeholders described above, worked to refine the concept. Breakout session sub-groups were led by not only NIST, but other federal agencies, representatives of industry, SDOs, and included international community representatives.

- The **November event served as a program initiation phase** decision milestone for the NIST Cloud Computing program in terms of gauging public support, interest and the appropriate planning and execution level going forward. In the November and early December timeframe, NIST completed it project planning, including milestone and internal resource allocations (n.b. the ***Strategy to Develop a USG Cloud Computing Technology Roadmap*** projects are level of effort activities which rely directly and heavily on public and private sector partners to take ownership of key activities and contributions to deliverables).

- The program planning phase, including establishment of public working groups and sub-groups, was completed December 2010 through March 2011. Several activities were initiated in parallel during this time period. Full execution began as planned, at the end of March 2011, marked by a third **Cloud Computing Forum and Workshop in April 2011**.

- The **target for the first draft USG Cloud Computing Technology Roadmap Interagency Report is October 2011.**

- The program will assess results, and assuming positive progress and continued support, plan and execute iteratively and incrementally starting in November 2011, until such time as its objectives are met.

6.0 How NIST is Measuring Success:

Performance is measured by completion of the milestones listed below.

Success metrics are: 1) the extent to which the deliverables from the program are used by the cloud computing community, and 2) the extent to which stakeholders continue to find the work useful and therefore continue to "vote with their feet" and remote participation in working groups and collaborative work.

7.0 Work and Products

7.1 USG Cloud Computing Technology Roadmap

The primary strategic deliverable of the NIST Cloud Computing program is the USG Cloud Computing Technology Roadmap which will be issued as an Interagency Report (IR).

- The roadmap is the mechanism that will be used to define and communicate the prioritized requirements that must be met to support the secure and effective USG adoption of cloud computing services, given the various deployment and service models. The roadmap will list of security, interoperability, and portability standards requirements, security guidance requirements, and related policy and technology requirements that have been identified as prerequisite to support USG Target Business Use Cases. The roadmap will provide context through the USG Target Business Use Cases and a neutral reference architecture and taxonomy.

- The Neutral Cloud Computing Reference Architecture and Taxonomy (high level conceptual architecture, taxonomy, and/or ontology is a frame of reference to facilitate communication, illustrate and understand various cloud services in the context of an overall Cloud Computing Model (to aid USG, industry and others in comparing "apples to apples" and to understand how various cloud services and components fit together by relating them to the reference architecture).

- As described above, the roadmap priorities will then be used to prioritize ongoing NIST tactical efforts (e.g. specific guidance development, generic technical standards use case, test, and specification development, or a particular desired prototype or pilot implementation). The roadmap also informs the broader IT community.

- This approach helps to ensure that Cloud Computing efforts are integrated, and to communicate and drive resolution of issues which inhibit and affect the application of Cloud Computing technology. The approach also facilitates integration with related initiatives such as cybersecurity and Health IT.

- In the December 2010 through March 2011 program initiation and planning phase, NIST, through the collaboration process and working groups, has identified major elements of the USG Cloud Computing Technology Roadmap. These include:

- 1) Cloud Computing Standards Roadmap, which is based on an inventory of Cloud Computing standards and leverages SDO and consortia work in defining cloud computing standards gaps;

- 2) Neutral Reference Architecture and Taxonomy which is a performance (requirements "what" as opposed to prescriptive "how" or vendor solution specific reference implementation) oriented logical and physical representation of cloud computing, based on a survey, analysis of, and leverages existing reference architectures work;

- 3) Relevant information captured through the USG Target Business Use Cases. These are designed to improve the overall USG cloud computing knowledge base by leveraging and sharing information and resources, and focus on mission operational requirements so that these can be translated into specific cloud security, interoperability, and portability technology requirements;

- 4) Cloud Computing Security Roadmap which is a prioritized list of cloud computing security requirements, categorized into USG operational requirements (input to Federal CIO Council Cloud Computing Advisory Council Security Working Group,) policy requirements (for hand-off to policy makers,) security standards and guidance priorities (used by NIST and others), and technology requirements (R&D, Industry).

7.2 Interim Deliverables & Useful Information for Cloud Adopters

In parallel with the development of USG Cloud Computing Technology Roadmap, the NIST Cloud Computing Strategic Program public working groups and associated NIST projects complete interim deliverables. These include products, information, and outreach activities which further the discussion and knowledge base of Cloud Computing. This work is made publically available through the NIST ITL Cloud Computing Website under "Useful Information for Cloud Adopters". Interim progress to date and short term plans are described in the Progress section below.

7.3 Requirements which fall out of Scope

Generation of the USG Cloud Computing Technology Roadmap is NIST led and facilitated. The USG Cloud Computing Technology Roadmap also serves as a communication vehicle to those who work on the requirements outside of the scope of the NIST mission. The roadmap list of priorities constitute a hand-off, and a transition to tactical efforts which fall under the mission and scope of many different organizations.

The expectation is that the administrative execution process to communicate, coordinate and track the tactical efforts which fall outside of the NIST Cloud Computing Program scope, including collaborative efforts, such as policy implementation, procurement related activities, or US government agency prototype and pilot projects, will be completed under the auspices of the Federal CIO Council, GSA Cloud Computing Program Management Office, and other organizations as appropriate.

8.0 Guiding Principles and Assumptions -- Process and Stakeholders

8.1 *Process*

The NIST Cloud Computing strategic program and working group processes are consistent with the NIST Health IT, Smart Grid and other NIST program and stakeholder approaches – adapted for the program scope and authorities.

The work is NIST led and facilitated through open public stakeholder meetings, and working groups are created through an open public invitation process. Academia, industry, SDOs, consortium, the international community as well as federal, state, and local governments actively participate and contribute as is consistent with the case of NIST work which is reviewed through the public comment process. However, in addition, stakeholders may lead sub-groups and participate in the development of these deliverables in addition to commenting on draft releases.

For consistency and continuity, NIST uses the NIST Cloud Computing Definition as a basis for context via the performance based neutral reference architecture and taxonomy.

All deliverables created from the NIST Strategy to Build a USG Cloud Computing Technology Roadmap are public domain deliverables. These correlate to but do explicitly include or reference more detailed industry, SDO and other specific architecture and service reference implementations.

Certain commercial entities, equipment, or materials may be identified in the deliverables of NIST Cloud Computing Program in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

The process of generating the USG Cloud Computing Technology Roadmap is one of iteratively translating, defining, and tracking the progress of Cloud Computing Priorities. In concept, this is represented by Step 3 of the Strategic

NIST Cloud Computing program – the process matches the requirements for US government cloud computing adoption (which have been defined using operational use cases from real Business Use Case examples) to Cloud Computing candidate security, interoperability, and portability candidate standards and reference implementations that address them, using a neutral, evolving, taxonomy and reference architecture as a tool for communication and analysis.

A strength of this process is the ability to broadly but specifically "nail down" the real and perceived concerns and issues, and to leverage the real world experience of the USG CIO community in terms of challenges, and the real world industry, SDO and practitioner experience and skills in order to analyze the requirements and potential solutions.

An advantage of this process is the ability to broadly identify requirements which must be satisfied to support USG adoption of Cloud Computing and to integrate them with tactical efforts beyond the scope of the individual participants (i.e. beyond standards, beyond security guidance.)

However, it is important to understand that this process is not a single point in time, single activity, specific working group or entity domain. The process of synthesizing the information and identifying the gaps in cloud computing standards, technology, and guidance is necessarily a "messy" and often unstructured process. This is driven by several factors: subject matter expertise, sheer numbers of participants, information, and experience, the volatility and rapid changes in technology and deployment state, and the incremental and iterative nature of the process. For purposes of grappling with these variables, NIST is using the roadmap document as the mechanism to focus this process and communicate the results.

8.2 External Partners and Stakeholders

The NIST Cloud Computing Program includes, but is not limited to these federal government sponsors and partners: United States Chief Information Officer, Federal Chief Information Officers' Council, DOC Census/ITA/NOAA, DoD/DISA, DOE, DHS, Office of Management and Budget, General Services Administration, NASA/AMES/CIO/GSFC/JPL, USAID, laboratories such as JPL, and the U.S. Government's Networking and Information Technology Development Program. The program also collaborates with the European Commission, Japan, National Association of State CIOs, and local government agencies such as the MD DOT.

The program collaborates with Standards Development Organizations, including but not limited to ISO, ANSI, DMTF, IEEE, IETF, OASIS, OCC, OGF, and others, and their members through professional organizations.

The program collaborates with industry and consortia including but not limited to Amazon, Microsoft, BSA, Red Hat, CA Technologies, Centuric, COSA, CSA, CISCO, EMC, Google, ITIC, Intel, NIST ISPAB, Oracle, SIIA, SNIA, Salesforce, South Florida Technology Alliance,Tech America, Vmware, and the WEF.

9.0 NIST Cloud Computing Projects & Working Groups' Interim Progress as of April 2011

9.1 Define US Government Target Business Use Cases

The mission of this project and working group is to define USG Target Business (mission) Use Cases which include: definition of a candidate agency system or service for the Cloud Computing model option; list of perceived risks, concerns, questions, issues; and operational scenario (scope to be determined; sufficient but not necessarily limited to focus security, interoperability, and portability requirements.)

The Target USG Cloud Computing Business Use Cases are a set of candidate deployments to be used as examples for various Cloud Computing model options, and identify realistic risks, concerns and constraints (i.e. a candidate deployment might be employee email and office automation or migration of a specific application system to a specific cloud computing model option.)

Agency programs are used to leverage existing effort and ensure real and practical focus. This is a very simplified view, and there are many possible categorizations of Cloud Computing model options, and many candidate agency systems and services for cloud services. The goal is to focus on an initial set in order to identify and focus on tangible, but high priority requirements in order to establish a focused starting point for resolution. The intent is to leverage agency efforts and deliverables – not to create unique work and deliverable requirements.

In addition to the Public Working Group, there is a second avenue of USG agency participation that falls under the cognizance of the Federal CIO Council sponsored Cloud Computing Advisory Council Standards Working Group and others as defined by the CCAC. Agencies provide Program Manager, CTO, and Engineering representatives who have the role of stakeholder for a given candidate cloud computing application. These individuals may lead a Working Group to develop a particular Business Use Case definition effort. Under the CCAC Standards Working Group the process may only be open to federal, state, and local agencies. NIST serves in the role of collaborator with the broader IT community with a common interest through the public working group, cognizant of the need to avoid sensitive subject matter.

There is not an explicit intent to select use cases by category, but there is an expectation that they can be categorized by service and deployment models.

	Software as a Service	Platform as a Service	Infrastructure as a Service
Public Deployment	X	X	X
Hybrid Deployment	X	X	X
Community Deployment	X	X	X
Private Deployment	X	X	X

- **Target Business Use Cases** include but are not limited to this initial set which is accessible through the NIST Cloud Computing collaboration site:

  - Generic VDI Business Use Case
  - FGDC GeoSpatial PaaS Business Use Case
  - USAID VDI Business Use Case
  - USAID Applications Business Use Case
  - STIDS Incident Response Business Use Case

  - **Characterization: NIST USG Target Business Use Case Working Group**

    - **Charter date** – January 2011; **Kickoff Meeting** – January 2011
    - **Deliverable** – Target Business Use Case templates; populated use cases; references
    - **Format** – weekly 1-hour teleconference meetings; one-one meetings with USG agencies and other stakeholders
    - **Participation** – 520 registrants; more than 245 organizations; 20 to 40 active meeting participants; established 4 subgroups to focus on key WG objectives and tasks
    - **Approach: 1)** Identify and document use case commonalities; 2) continue to evolve use case development process; 3) identify gaps and roadblocks to implementation; 4) Draft and finalize use case document to feed USG Cloud Roadmap

9.2 Define Neutral Reference Architecture

The mission of this project and working group is to define a Neutral Cloud Computing Reference Architecture and Taxonomy – a high level conceptual architecture and taxonomy which can be used as a frame of reference to facilitate communication, illustrate and understand various cloud services in the context of an overall Cloud Computing Model (to aid USG, industry and others in

comparing “apples to apples” and to understand how various cloud services and components fit together by relating them to the reference architecture).

The approach is generally to expand the NIST Cloud Computing Definition and develop a consistent reference architecture and taxonomy as public domain deliverables, which may correlate to, but not necessarily include or explicitly reference more detailed industry, SDO and other specific architecture and service reference implementations. The expectation is that these deliverables will evolve as the technology evolves.

In only three months NIST and the working group have surveyed ten existing reference architecture models, synthesized an approach, and contributed meaningfully to expand the existing reference architecture models to further define and improve the understanding of cloud computing:

a) added/defined the concept of carrier, broker and auditor roles and the associated functions,

b) identified and defined the Resource abstraction and control layer that could be supported by innovation to convert the pools of hardware resources into cloud ready resources -- cloud services (identified by the five characteristics in the NIST cloud definition) can be offered (on top of these abstract resource layers),

Proposed an answer to a common question of bias toward vendors using hypervisor/VM technology/solutions, by accommodating companies that provide their cloud services on top of hardware without the common technology such as hypervisor and VM (example: Google and some high performance computing solutions),

c) More properly describe the SAAS, PAAS and IAAS service models to clarify that they are not necessarily layered (ie. SAAS does not have to be running/offered on top of PAAS, Vendor could offer PAAS without IAAS,) and

d) Clarified a key point of discussion for understanding the relationship of security and privacy in the context of cloud computing which applies across all layers of the cloud computing logic model (e.g.,physical, resource abstraction and service layers).

- **Survey and Assessment of Cloud Computing Reference Models**

  The survey and assessment is available through the NIST Collaboration site. The assessment characterizes, compares and analyzes the differences in the models, including but not limited to those proposed by known cloud organizations, providers and federal agencies. These include the Cloud Computing Use Case Discussion Group, Distributed

Management Task Force, Cloud Security Alliance, IBM Cloud Reference Architecture, GSA: Federal Cloud Computing Initiative, Cisco Cloud Reference Architecture Framework Open Security Architecture: Secure Architecture Models, SNIA standard: Cloud Data Management Interface, and Elastra: A Cloud Technology Reference Model for Enterprise Clouds.

- **Reference Architecture and Taxonomy documents**

  These documents, currently in draft are complementary to work being completed in other project and working group efforts.

  - NIST CCRATWG 029: **NIST Coud Computing Reference Architecture Model completed (3/30/11)**
  - NIST CCRATWG 030: **NIST Cloud Taxonomy, version 1.0, updated 03/31/2011.** (mm format)
  - NIST CCRATWG 031: **NIST Cloud Taxonomy Terms and Definitions, version 1.0, updated 03/31/2011**

  - **Value added:**
    i. Added/defined the concept of carrier, broker and auditor roles and the associated functions.
    ii. identified and defined the Resource abstraction and control layer
    iii. Described the SAAS, PAAS and IAAS service models to show that they are not necessarily layered
    iv. Identified Privacy and Security in the RA as separate but applying to all levels of cloud computing

  o **projected deliverables in FY 2011 are:**

    - Version 2.0 of NIST Cloud Computing Reference Architecture which includes a more detailed description of security and privacy.
    - Version 2.0 of NIST Cloud Computing Taxonomy which includes
      - Security & Privacy
      - Updated SaaS taxonomy to reflect USG Business Use Cases.
      - Newly identified additional taxonomies to support USG Business Use Case
    - Document – NIST Cloud Computing Reference Architecture Analysis of USG Target Business Use Cases

- Document – NIST Cloud Computing Reference Architecture Analysis of current cloud standards.

- **Characterization: Reference Architecture (&Taxonomy) working group**

  - **Charter date** – Janurary 2011; **Kickoff Meeting** – January 2011
  - **Deliverable** – Neutral Reference Architecture conceptual model & Taxonomy
  - **Format** –weekly 1-2-hour teleconference meetings;
  - **Participation** – 499 registrants; more than 215 organizations; members include but are not limited to US Army, usdoj, nasa, nara, nsa, DHS, DOT, EMC, GSA, ATT, amazon, ca techonologies, cisco,HP, IBM, intel, microsoft, oracle, vmware, virtualglobal, TmForum, IEEE, cloud security alliance, TechAmerica, john hopkins univ, deloitte, fujitsu, SAIC, BAH, etc
  - **Approach: 1)** bi-weekly meetings alternating between RA and Taxonomy ; 2) next iteration of RA; 3) Privacy and Security aspects of RA (as determined by Security working groups; 4) revisit data as a Service ; 5) Identify additional needed Taxonomies; 6) initiate Cloud Computing full Ontology

9.3 NIST Cloud Computing Standards Roadmap Working Group:

The mission of this working group is to survey the existing standards landscape for security, portability, and interoperability standards / models / studies relevant to cloud computing, determine standards gaps, and identify standardization priorities.

- **Inventory of Standards Relevant to Cloud Computing**

  The inventory is made available through the NIST Collaboration site. The inventory assembles the highest-level protocols, definitions and standards that are applicable widely to the cloud computing use cases identified in the scope of the complementary Cloud Computing strategic and tactical projects and working groups.

  The intent is expand the set and classify it according to the taxonomical hierarchy defined by the NIST Reference Architecture and Taxonomy project and working group, and to supplement this categorization using tags to indicate other areas of applicability for a given standard.

- **CC Standards Roadmap**

  This document, currently in draft, provides context using the NIST Cloud Computing Definition, Reference Architecture and other working group

efforts. Based on the NIST standards inventory, the NIST conceptual model, and the USG requirements for cloud computing (from information gleaned from the Use Case and SAJACC working groups), the NIST team is working on defining cloud computing standards gaps and priorities. The first edition of the Standards Roadmap is targeted for the end of April 2011.

4. **Characterization: Cloud Computing Standards Roadmap Working Group**

    - **Charter date** -- December 2010; **Kickoff Meeting** – January 2011
    - **Deliverable** – A recommended Cloud Computing Standards Roadmap document
    - **Format** – initially weekly 2-hour teleconference meetings; currently every two weeks
    - **Participation** – 520 registrants; more than 245 organizations; 20 to 40 active meeting participants; NIST is also participating in SDOs with cloud computing activities, such as IEEE, DMTF, OGF, SNIA, TM Forum, INCITS DAPS38, ITU-T, and ISO/IEC JTC 1/SC 38.
    - **Approach: 1)** Start with the NIST Cloud Computing definition; 2) Leverage the work of the other NIST Working Groups and others; 3) Build an inventory of standards; 4) Map security, portability, and interoperability standards to USG requirements & NIST conceptual model; 5) Look for standards gaps and overlaps; and 6) Identify USG standardization priorities.

9.4 Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC) project and working group

SAJACC was conceived to support cloud computing adoption in the interim period between the emergence of cloud computing technology and the point where security, portability, and interoperability standards are formalized.

The SAJACC process is designed to support the definition of generic technical security, portability, and interoperability requirements through use case methodology, the development of test plans and procedures using validation criteria drawn from the use cases, and to disseminate this information along with the results of the test execution against “reference” cloud implementations (which incorporate candidate interface specifications.)

SAJACC focuses on facilitating performance based (as opposed to design based) standards development in order to support and not limit innovation.

- **SAJACC Portal**: was launched September 2010

- **SAJACC generic technical interoperability, security and**

portability use cases were completed November 2010. The project vetted these with cloud computing stakeholders in academia, government, and industry. SAJACC will continue to update its public Internet-accessible repository of cloud computing usage scenarios (i.e., use cases), documented cloud system interfaces, pointers to cloud system reference implementations, and test results showing the extent to which different interfaces can support individual use cases.

- **SAJACC Testing Proof-of-concept** was initiated in February 2011. SAJACC identified an initial set of candidate legacy cloud system interfaces, along with their reference implementations, to complete proof of concept validation of the SAJACC process by providing publically available test drivers.

Project document deliverables to date are:

- **Cloud Computing Use Cases**: a set of 25 generic technical use cases that seek to express selected portability, interoperability, and security concerns that cloud users may have (referenced above, and posted on the SAJACC Portal in November 2010)
- **Cloud Interface Catalogu**e: a set of known cloud interfaces 9specification sets an APIs), initiated January 2011
- **SAJACC Use Case Test**: referenced above, test drive code and packages to implement SAJACC use cases (posted source code for all use case test drivers on the NIST public twiki, February 2011)

Significant contributions:

- completed with community involvement and included surveying 10 appropriate cloud system interfaces
- collaboration has occurred with the cloud and grid communities, with active participation from OGF, DMTF, Oracle, and Microsoft (Microsoft has used the NIST SAJACC project source code to implemented a number of our SAJACC use cases on Azure)
- developed a use case test driver framework
- proven with three cloud computing system interfaces of broad interest (S3, EC2, CDMI) to implement test drivers for 7 use cases
    - UC 3.4 (copy data objects into a cloud)
    - UC 3.5 (copy data objects out of a cloud)
    - UC 3.6 (erase data objects in a cloud)
    - UC 5.7 (sharing access to data in a cloud)
    - UC 4.1 (copy data between clouds): March 15
    - UC 3.7 (allocate VM instance): March 22
    - UC 3.8 (manage VM instance state): March 29
- identified several key issues so far: erase data object limitations,

- central importance of identity management for cloud interoperability, and essential similarities in the semantics of key cloud IaaS interfaces

- **Characterization: SAJACC Working Group**

    - **Kickoff Meeting** – January 2011
    - **Deliverable** – Populated SAJACC portal and processes
    - **Format** –weekly 1-2-hour teleconference meetings
    - **Participation** – 250 registrants; more than 114 organizations; including but not limited to Amazon, att, bah, ca technologies, census, cisco, cloud security alliance, dhs, disa mil, doc, doe, faa, fujitsu, gsa, hp, ibm, intel, microsoft, nasa, ncsc mil, oracle, OGF, redhat, symantec, tmforum, usda, vmware, virtual global, etc
    - **Approach: 1**) implement remaining Use Cases Document (14); 2) augment use cases with Identity Management (targets interoperability); 3) re-implement use cases with more of the 10 known IaaS interfaces; 4) more cross-implementation experiments; 5) especially, VM migration experiments across diverse VM technologies (data formats such as OVF); 6) introduce use cases in PaaS offerings (as well as IaaS); 7) expand the test driver infrastructure to mix/match multiple use cases + interfaces + providers, driven by configuration settings.

9.5 *Koala*: Measurement Science for Complex Information Systems

This project is applying modeling and analysis techniques for complex systems to compare resource-allocation algorithms for on-demand IaaS clouds. The project has two main objectives: (1) assess the effectiveness of various modeling and analysis techniques and (2) provide insights into resource-allocation algorithms for IaaS clouds. The project team is multidisciplinary: (computer science), (statistics), (math) and (infoViz).

FY 2011 Completed Deliverables

- Nov. 2010 – Developed ***Koala***, a discrete-event simulation model of IaaS clouds, inspired by the Amazon Elastic Compute Cloud and the Eucalyptus open-source cloud software.
- Dec. 2010 – Completed information visualization software that animates the global dynamics of ***Koala*** and that allows experimenters to explore system behavior.
- Jan. 2011 – Completed sensitivity analysis that identifies the essential dynamic behaviors of ***Koala*** and the model parameters that significantly influence those behaviors.

- Apr. 2011 – Completed a Markov chain model derived for ***Koala***. The Markov chain model will be used to identify and characterize potential failure scenarios that can cause performance collapse in on-demand IaaS clouds.

FY 2011 Planned Deliverables -- Sep. 2011 – Complete a comparison of 18 potential resource-allocation algorithms for on-demand IaaS clouds. This comparison will consider a cloud operating under nominal conditions, as identified by the previous sensitivity analysis.

Public Collaboration: The Koala project does not host a public working group, although it does share the results of its work publically and solicit comments. The Koala work is available through the NIST Cloud Computing Program website, and demonstrated in the NIST Cloud Computing Forum and Workshop (April 2011.)

9. 6 Cloud Security: Technical Advisory role to the Federal CIO Council Cloud Computing Executive Steering Committee and Cloud Computing Advisory Council

Much of the NIST security work to date has been in the arena of guidance:

- NIST released a special publication on virtualization security guidance SP 800 -125, DRAFT *Guide to Security for Full Virtualization Technologies*, July 2010; revised Dec 2010

- SP 800 – 144, DRAFT *Guidelines on Security and Privacy Issues in Public Cloud Computing,* Jan 2011

- SP 800 – 145, DRAFT *Cloud Computing Definition*, Jan 2011

- NIST provided technical support for the draft interpretation of FISMA security controls for cloud computing services which was issued by the Federal Risk Authorization and Management Program (FedRAMP), through the the GSA led FedRAMP program office in November 2010. NIST has continued in the role technical advisor in the refinement of the FedRAMP project.

As in the case of the USG Cloud Computing Target Business Use Cases, in addition to the Security Public Working Group, there is a second avenue of USG agency participation that falls under the cognizance of the Federal CIO Council sponsored Cloud Computing Advisory Council Security Working Group and others as defined by the CCAC. Key government collaborators include but are not limited to the FedRAMP CISO membership, ISIMC, DOC Cyber Security Task Force and OCIO, NASA, DOD/DISA, DHS, Department of State, and

National Geospatial community. Under the CCAC Standards Working Group and other federal efforts, the process may be appropriately opened to only other agencies, and state and local governments. NIST serves in the role of collaborator with the broader IT community with a common interest through the public working group, cognizant of the need to avoid organization sensitive subject matter.

- **Characterization: Cloud Security Working Group**

    - **Charter & Kickoff Meeting** – February 2011
    - **Deliverable** – Set of high priority Cloud Computing security requirements for standards, guidance, and technology in the form of a Cloud Computing Security Roadmap sub-section of the broader USG Cloud Computing Technology Roadmap
    - **Format** –weekly 1-2-hour teleconference meetings
    - **Participation** – 557 registrants; more than 252 organizations; including but not limited to Amazon, US Army, ATT, CA Technologies, CISCO, CSA, DHS, DOC, DOT, OMB, Fujitsu, GSA, HP, IBM, IEEE, Intel, Johns Hopkins Univ, Microsoft, NARA, NASA, US Navy, NCSC, Nsa, Oracle, Qwest, Redhat, Symantec, Tmforum, UIUC, USDA, DOJ, Vmware
    - **Approach: 1**) identify set of high priority cloud computing security concerns through use cases and participant submissions; 2) explore and prioritize through adopter and provider collaboration; 3) use list to inform NIST guidance priorities; 4) communicate externally through roadmap

10.0 Beyond 2011 -- NIST Cloud Computing Program

As described initially, the expectation is that the NIST Cloud Computing program, including the Strategy to Build a USG Cloud Computing Technology Roadmap will be assessed annually and re-planned based on the overall NIST mission and priorities.