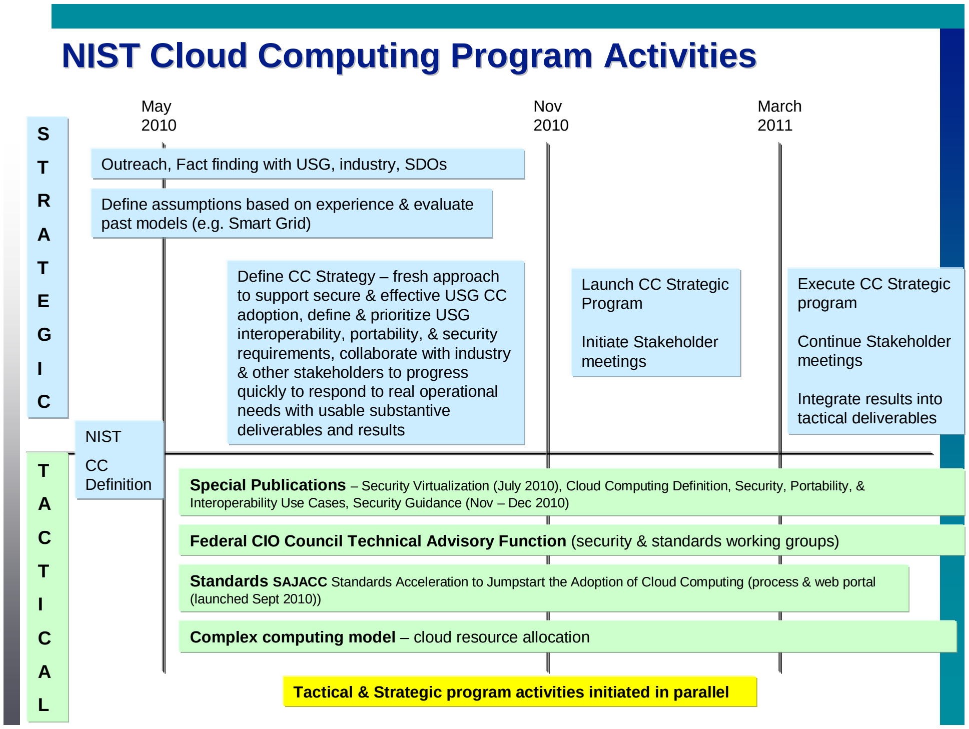
NIST Cloud Computing Program Overview

The NIST Cloud Computing Program includes Strategic and Tactical efforts which were initiated in parallel, and are integrated as shown below:



NIST Cloud Computing Program Activities

May 2010

Nov 2010

March 2011

STRATEGIC

Outreach, Fact finding with USG, industry, SDOs

Define assumptions based on experience & evaluate past models (e.g. Smart Grid)

Define CC Strategy – fresh approach to support secure & effective USG CC adoption, define & prioritize USG interoperability, portability, & security requirements, collaborate with industry & other stakeholders to progress quickly to respond to real operational needs with usable substantive deliverables and results

Launch CC Strategic Program

Initiate Stakeholder meetings

Execute CC Strategic program

Continue Stakeholder meetings

Integrate results into tactical deliverables

NIST CC Definition

TACTICAL

Special Publications – Security Virtualization (July 2010), Cloud Computing Definition, Security, Portability, & Interoperability Use Cases, Security Guidance (Nov – Dec 2010)

Federal CIO Council Technical Advisory Function (security & standards working groups)

Standards SAJACC Standards Acceleration to Jumpstart the Adoption of Cloud Computing (process & web portal (launched Sept 2010))

Complex computing model – cloud resource allocation

Tactical & Strategic program activities initiated in parallel

<u>Rationale for launching strategic and tactical efforts in parallel</u>

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

- developing technical and security guidance by starting with a foundation of the 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 validate interface specifications, and
- modeling complex computing models.

There is no reason to delay the initiation of these tactical steps – they are always necessary and effective in supporting the development of a new technology model and transforming operational information systems to apply the model.

However, at the same time, a strategy, which is formed based on an understanding of the highest priority mission oriented requirements and issues which must be addressed to apply the technology, is needed to focus these tactical efforts in order to ensure that they best use scarce resources and address most important requirements first.

In this context, under the guidance of the United States Chief Information Officer and Director 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.

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

After launching its first Cloud Computing Forum and Workshop in May 2010 to expand stakeholder outreach, NIST sought and considered the opinions and requirements expressed by federal, state, and local governments, standards development organizations, industry, the international community, and other IT community stakeholders. NIST has also considered what it has learned through initiatives such as the Smart Grid Strategy and Roadmap program, and has developed and is proposing a strategy which is described below.

What NIST Has Learned

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 model delivery options (private, public, community and hybrid) and service options (software, platform, and infrastructure), and to provide guidance for and make risk based decisions. This is needed to get past the polarization of two end of the spectrum solutions – 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.

Optimally, there would be sufficient information to analyze and write guidance – a "rule book" for cloud computing that agencies could read which provides prescriptive guidance. A rule book that would remove the uncertainty in decision making BEFORE cloud computing is deployed.

However, the nature of an emerging technology such as the cloud computing model is such that there is insufficient 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 amount of information that is known. Some set of 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. Much the known experience relates to infrastructure services because this is 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 be feasibly developed (as compared to the case of a mature technology model.) In other words, we need to develop guidance given the reality of the constraints that an emerging technology model creates.

NIST also 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. The need is for a performance based reference architecture that is more detailed than the broadly used NIST Definition of Cloud Computing, in order to help the federal CIO community understand and categorize various cloud offerings, but abstract to a high enough level that it does not assume or "lock in" a specific vendor solution reference implementation. This is needed to ensure that innovation is not constrained, to ensure a level playing field for all stakeholders – vendors, nation states, and standards bodies. The goal is to define a neutral reference architecture that can be used 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.

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.

Strategic Approach

Goal:

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

Timeline:

As shown on the NIST Cloud Computing Program Activities figure and described above, May through November 2010, NIST listened to industry stakeholders and developed the concept of a collaborative strategy which is outlined below.

In its November 2010 Cloud Computing Forum and Workshop II, which included a broad set of formal agenda as well as attendee participants, NIST publically presented the concepts of the ***NIST Strategy to Develop a USG Cloud Computing Roadmap***. The strategy was received positively by the stakeholder community. In the same November 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 sessions sub-groups were led by not only NIST, but other federal agencies, representatives of industry, SDOs, and included international community representatives.

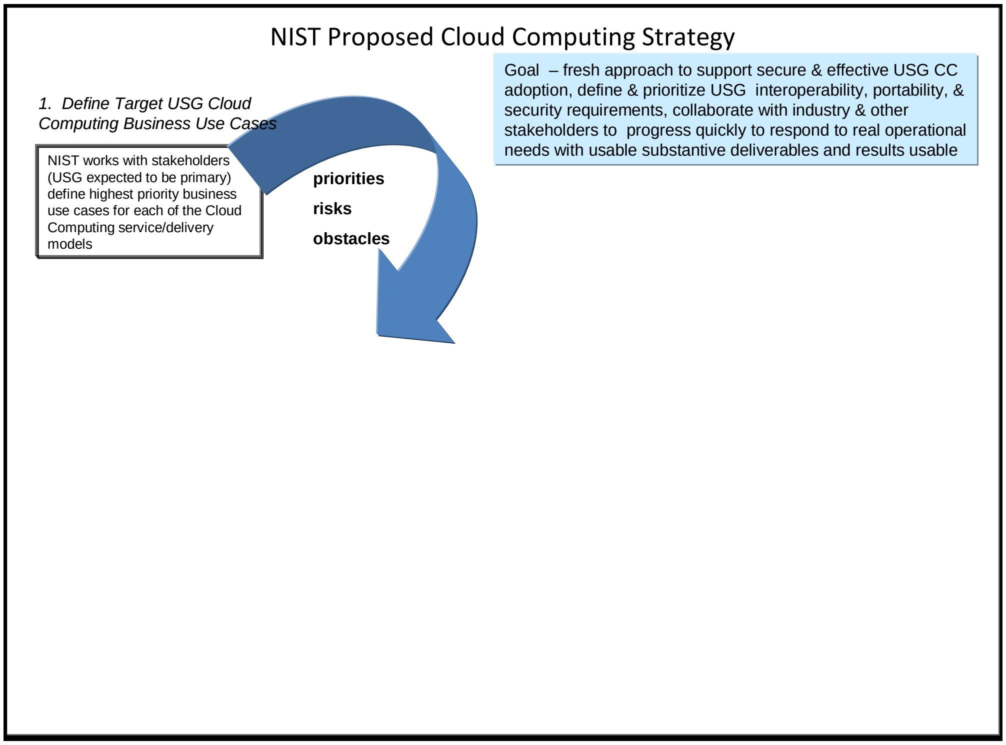
The November event served as a program initiation phase decision milestone for the NIST Cloud Computing program in terms of gauging public support, interest and the appropriate planning and execution level going forward. In the November and early December timeframe, in response to and directly based on the enthusiastic and voluntary participation and support level, NIST completed it project planning, including milestone and internal resource allocations (n.b. the ***Strategy to Develop a USG Cloud Computing Roadmap*** projects are level of effort projects 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, is targeted for December 2010 through March 2011. While some activities will be initiated in parallel during this time period, full execution is targeted to begin at the end of March 2011, marked by a third Cloud Computing Forum and Workshop in or around April 2011. The target for the first draft USG Cloud Computing Roadmap deliverable document is October 2011. The expectation is that the program will assess results, and assuming positive progress and continued support, executive iteratively and incrementally starting in November 2011, until such time as its objectives are met. Success and completion metrics will be defined in the initial project planning phase which ends in March 2011.

Processes and Methodology :

The proposed method to implement the NIST led collaborative Strategy ***to Develop a USG Cloud Computing Roadmap*** is to:

1) Define Target USG Cloud Computing Business Use Cases (set of candidate deployments to be used as examples) identified and led by key US government agencies to identify realistic risks, concerns and constraints which will translate into interoperability, portability and security requirements. (i.e. a candidate deployment might be employee email and office automation or migration of a specific application system such as US patent applications, Census applications, NOAA Weather Service applications, DISA applications to a specific cloud computing model option – n.b. these are hypothetical candidate options.)



NIST Proposed Cloud Computing Strategy

Goal – fresh approach to support secure & effective USG CC adoption, define & prioritize USG interoperability, portability, & security requirements, collaborate with industry & other stakeholders to progress quickly to respond to real operational needs with usable substantive deliverables and results usable

1. Define Target USG Cloud Computing Business Use Cases

NIST works with stakeholders (USG expected to be primary) define highest priority business use cases for each of the Cloud Computing service/delivery models

The expectation is that this process will leverage existing and proposed agency cloud computing efforts, improving the overall USG cloud computing knowledge base by leveraging and sharing information and resources, and serving as a catalyst to focus on mission operational requirements.

Deliverable (for illustration and discussion):

For consideration, there are several working group, sub-group and deliverable approaches, which are all candidates for parallel and complementary efforts:

One option, suggested in the November 2010 workshop is a “story based” approach – traditional concept of operations approach to defining the key requirements for one or more of the examples above.

Another option, also suggested in the November 2010 workshop is a “common” function approach, such as defining key functional requirements which must be met in cloud computing model services such as critical mission search or geospatial functions.

Another option, also suggested in the November 2010 workshop, is focus on broad common cloud computing options such as office automation/email applications.

The expectation is that these target Cloud Computing Business Use Cases will map to various Cloud Computing service model and deployment model options:

	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

Each Business Use Case includes: 1) 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.)

Granted, 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. The goal is to establish a focused starting point for resolution.

Participant Roles (for illustration and discussion):

The effort as proposed is NIST led and facilitated. USG agency participation shall be under the cognizance of the Federal CIO Council sponsored Cloud Computing Advisory Council Standards Working Group and others as defined by the CCAC. Agencies will provide Program Manager, CTO, and Engineering representatives who have the role of stakeholder for a given candidate cloud computing application to lead a Working Group to develop a particular Business Use Case definition effort. The process may be opened to only other agencies, as well as the broader IT community with a common interest (e.g. state and local governments, financial and healthcare sectors.) Agency programs are used to leverage existing effort and ensure real and practical focus.

The intent is to leverage agency efforts and deliverables – not to create unique work and deliverable requirements.

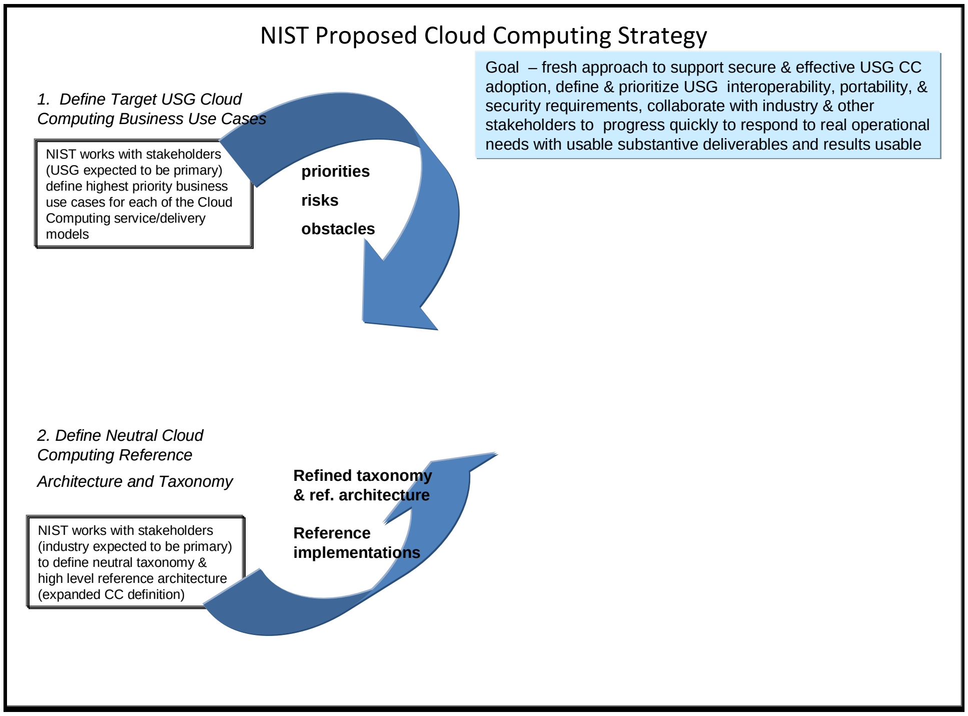
2) In parallel with Step 1:

Define Neutral Cloud Computing Reference Architecture and Taxonomy (high level conceptual architecture, taxonomy, and/or ontology 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).

Deliverable (for illustration and discussion):

One deliverable approach is to expand the NIST Cloud Computing Definition and develop a consistent performance based reference architecture and taxonomy (n.b.

all deliverables from the NIST Strategy to Develop a USG Cloud Computing Roadmap will be public domain deliverables, which will correlate to, but do explicitly include or reference more detailed industry, SDO and other specific architecture and service reference implementations.



NIST Proposed Cloud Computing Strategy

Goal – fresh approach to support secure & effective USG CC adoption, define & prioritize USG interoperability, portability, & security requirements, collaborate with industry & other stakeholders to progress quickly to respond to real operational needs with usable substantive deliverables and results usable

1. Define Target USG Cloud Computing Business Use Cases

NIST works with stakeholders (USG expected to be primary) define highest priority business use cases for each of the Cloud Computing service/delivery models

priorities

risks

obstacles

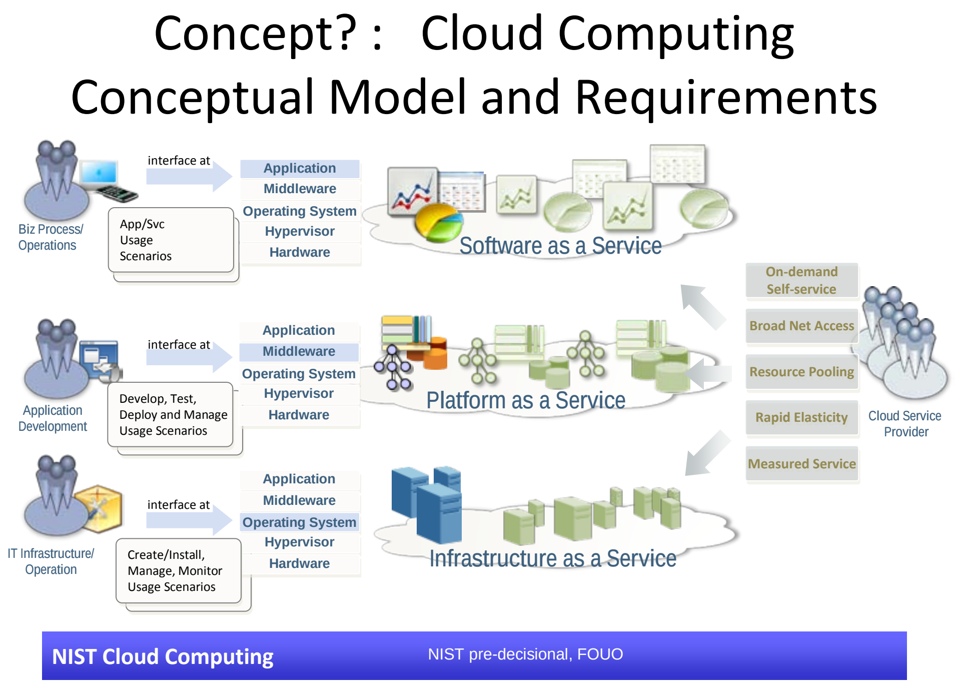
2. Define Neutral Cloud Computing Reference Architecture and Taxonomy

NIST works with stakeholders (industry expected to be primary) to define neutral taxonomy & high level reference architecture (expanded CC definition)

Refined taxonomy & ref. architecture

Reference implementations

The expectation is that these deliverables will evolve as the technology evolves. (i.e. expansion of the notional graphic below)



Concept? : Cloud Computing Conceptual Model and Requirements

NIST Cloud Computing NIST pre-decisional, FOUO

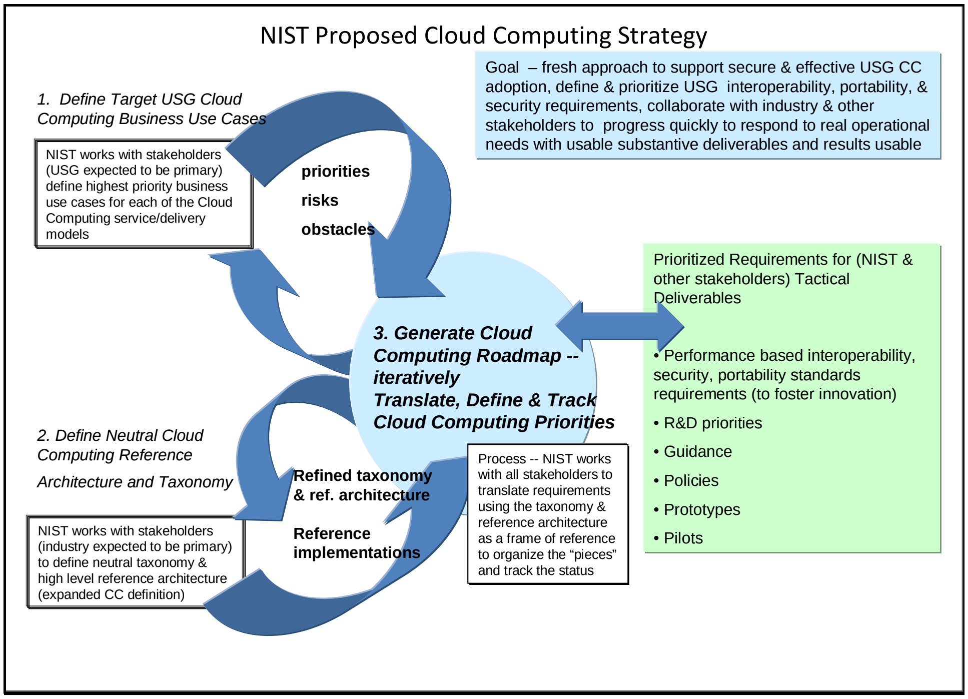
Participant Roles (for illustration and discussion):

The process as proposed is NIST led and facilitated through open public stakeholder meetings, and working groups created through an open public invitation process. The expectation is that industry, SDOs, consortium, as well as federal, state and local governments will actively participate and contribute (just as is currently the case through the public comment process.) However, similar to the Smart Grid program and stakeholder approach, stakeholders may lead sub-groups and participate in the development of these deliverables in addition to commenting on draft releases.

3) Iteratively, and incrementally as there is progress from Steps 1 & 2:

Generate Cloud Computing Roadmap – Iteratively Translate, Define & Track Cloud Computing Priorities

The Step 3 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.



NIST Proposed Cloud Computing Strategy

Goal – fresh approach to support secure & effective USG CC adoption, define & prioritize USG interoperability, portability, & security requirements, collaborate with industry & other stakeholders to progress quickly to respond to real operational needs with usable substantive deliverables and results usable

1. Define Target USG Cloud Computing Business Use Cases

NIST works with stakeholders (USG expected to be primary) define highest priority business use cases for each of the Cloud Computing service/delivery models

priorities

risks

obstacles

3. Generate Cloud Computing Roadmap -- iteratively Translate, Define & Track Cloud Computing Priorities

Prioritized Requirements for (NIST & other stakeholders) Tactical Deliverables

- Performance based interoperability, security, portability standards requirements (to foster innovation)
- R&D priorities
- Guidance
- Policies
- Prototypes
- Pilots

2. Define Neutral Cloud Computing Reference Architecture and Taxonomy

NIST works with stakeholders (industry expected to be primary) to define neutral taxonomy & high level reference architecture (expanded CC definition)

Refined taxonomy & ref. architecture

Reference implementations

Process -- NIST works with all stakeholders to translate requirements using the taxonomy & reference architecture as a frame of reference to organize the "pieces" and track the status

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

The cloud computing tactical efforts to date are appropriately geared to reducing uncertainty. However, these efforts are directed toward Cloud Computing from a general broad perspective. To more effectively support US government cloud computing adoption, the strategy narrows the focus more specifically identify highest priority government agency Cloud Computing requirements and direct the tactical resources to these priorities.

Deliverable (for illustration and discussion):

The overall deliverable is a Strategy and Roadmap for US Government Cloud Computing.

The strategy and roadmap document will include a prioritized US government list of security, interoperability, and portability standards requirements, security guidance requirements, and research & development priorities, needed prototypes, pilots, policies and potentially other required items that are prerequisite to satisfy a particular Business Use Case and Cloud Computing model option.

This list is then used to prioritize ongoing 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 list is by US government agencies, but also provides information to the broader IT community.

The expectation is that the list will be developed as part of the NIST led collaborative ***Strategy to Develop a USG Cloud Computing Roadmap***, but will be shared with the appropriate entities who are stakeholders and/or responsible for these areas, such as policy makers.

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, but are not necessarily solved by technology. The approach also facilitates integration with related initiatives such as cybersecurity and those which may utilize cloud computing (i.e. Health IT).

Participant Roles (for illustration and discussion):

As proposed, the neutral and core technical process to Generate the Cloud Computing Roadmap is NIST led and facilitated – up to the point of defining the Cloud Computing requirements in the form of tactical requirements. These deliverables 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, such as policy development or US government 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.

Tactical Approach

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. Progress in the tactical projects, which are complementary to and integrated with the strategic program is as follows.

Description and Timeline

In 2008-2009, NIST initiated a set of cloud computing activities. In May 2010, NIST increased its focus on and activity level of cloud computing, hosting a large public stakeholder *Cloud Computing Forum and Workshop.* NIST announced several tactical efforts geared, specifically, to support cloud computing standards acceleration and guidance development to support United States Government adoption of Cloud Computing, and has made progress on these efforts. In the November 2010 *NIST Cloud Computing Forum and Workshop II*, NIST provided an updated status on these efforts.

These efforts included developing guidance in the form of special publications and serving in a technical advisory role to the Federal CIO Council Cloud Computing Advisory Council. These security guidance efforts generally make use of and adapt the existing security measures to cloud. For example, NIST released a special publication on virtualization security guidance (SP 800-125) was published for comment in July 2010. A draft interpretation of FISMA security controls for cloud computing services was developed by the Federal Risk Authorization and Management Program (FedRAMP), and made available by the GSA led FedRAMP program office in November 2010. Additional cloud computing specific guidance is planned for draft public release in December 2010. Future special publication development includes guidance related to role and responsibility definition for cloud service providers and consumers. However, the ability to provide comprehensive and prescriptive "rule book" guidance is constrained because the technology is in an innovation stage and the installed experience base is still limited. (n.b. This is a major driver for the strategic approach as described above.)

NIST also announced and initiated the Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC), 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 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. The SAJACC website became publically available in September, 2010, and NIST initiated public comment and collaboration to refine the first series of generic technical use cases in November 2010.

Going Forward

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

Public stakeholder participation is encouraged. All parties are encouraged to sign up for working groups and to directly participate in the collaborative voluntary efforts and to directly contribute through the NIST ITL Cloud Computing website.