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

Special Publication 500-293
(Draft)

US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft)

High-Priority Requirements to Further USG Agency Cloud Computing Adoption

Lee Badger, David Bernstein, Robert Bohn, Frederic de Vaulx, Mike Hogan, Jian Mao, John Messina, Kevin Mills, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf

NIST Cloud Computing Program
Information Technology Laboratory

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

This page left intentionally blank

NIST Special Publication 500-293
(Draft)

US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft)

High-Priority Requirements to Further USG Agency Cloud Computing Adoption

Lee Badger, David Bernstein, Robert Bohn, Frederic de Vaulx, Mike Hogan, Jian Mao, John Messina, Kevin Mills, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf

---

Information Technology Laboratory

Cloud Computing Program
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

November 2011

U.S. Department of Commerce
John E. Bryson, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. This Special Publication 500-series reports on ITL's research, guidance, and outreach efforts in Information Technology and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 500-293 (Draft)

Natl. Inst. Stand. Technol. Spec. Publ. 500-293, 32 pages (November 2011)

Acknowledgments

The authors, David Bernstein, Jian Mao, and Jin Tong, of Knowcean Consulting Incorporated (under contract through the Federal Integrated Product Team, Space & Naval Warfare [SPAWAR] Systems Center Atlantic), Frederic de Vaulx of Prometheus Computing LLC (under contract), Lee Badger, Robert Bohn, Mike Hogan, John Messina, Kevin Mills, Annie Sokol, Fred Whiteside, and Dawn Leaf of the National Institute of Standards and Technology (NIST), gratefully acknowledge and appreciate the broad contributions from members of the NIST Cloud Computing USG Target Business Use Case, Reference Architecture and Taxonomy, Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC), Security, and Standards working groups.

We especially acknowledge Lisa Carnahan, Romayne Hines, Michaela Iorga, Mary Saunders, Terry Schwarzhoff, and James St. Pierre of NIST for providing editorial review and support.

We especially acknowledge Earl Crane, of the Department of Homeland Security and Information Security and Identity Management Committee (ISIMC), whose advice and technical insight assisted this effort.

We also wish to acknowledge the members of the Federal Cloud Computing Standards and Technology Working Group and other interagency contributors, listed in Appendix A of this document.

Additional acknowledgments will be added upon the final publication of this guideline.

This page left intentionally blank

Table of Contents

This page left intentionally blank

Executive Summary

The National Institute of Standards and Technology (NIST), consistent with its mission,[1] has a technology leadership role in support of United States Government (USG) secure and effective adoption of the Cloud Computing model[2] to reduce costs and improve services. This role is described in the 2011 *Federal Cloud Computing Strategy*[3] as "*... a central one in defining and advancing standards, and collaborating with USG Agency CIOs, private sector experts, and international bodies to identify and reach consensus on cloud computing technology & standardization priorities*."

This NIST Cloud Computing program and initiative to develop a *USG Cloud Computing Technology Roadmap* is one of several complementary and parallel USG initiatives defined in the broader *Federal Cloud Computing Strategy* referenced above.

The *Federal Cloud Computing Strategy* characterizes cloud computing as a "*profound economic and technical shift (*with*) great potential to reduce the cost of federal Information Technology (IT) systems while ... improving IT capabilities and stimulating innovation in IT solutions*."

In the technology vision of *Federal Cloud Computing Strategy* success, USG agencies will be able to easily locate desired IT services in a mature and competitive marketplace, rapidly procure access to these services, and use them to deliver innovative mission solutions. Cloud services will be secure, interoperable, and reliable. Agencies will be able to switch between providers easily and with minimal cost, and receive equal or superior services.

Decision makers contemplating cloud computing adoption face a number of challenges relating to policy, technology, guidance, security, and standards. Strategically, there is a need to augment standards and to establish additional security, interoperability, and portability standards to support the long-term advancement of the cloud computing technology and its implementation. Cloud computing is still in an early deployment stage, and standards are crucial to increased adoption. The urgency is driven by rapid deployment of cloud computing in response to financial incentives. Standards are critical to ensure cost-effective and easy migration, to ensure that mission-critical requirements can be met, and to reduce the risk that sizable investments may become prematurely technologically obsolete. Standards are key to ensuring a level playing field in the global marketplace.

Recognizing the significance and breadth of the emerging cloud computing trend, NIST designed its program to support accelerated US government adoption, as well as leverage the strengths and resources of government, industry, academia, and standards organization stakeholders to support cloud computing technology innovation.

---

[1] This effort is consistent with the NIST role per the National Technology Transfer and Advancement Act (NTTAA)

[2] *NIST Definition of Cloud Computing*, Special Publication 800-145 (Draft) "Cloud computing is a model for enabling ubiquitous, 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] Office of Management and Budget, U.S. Chief Information Officer, *Federal Cloud Computing Strategy*, Feb. 8, 2011. Online: www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.

Framing the Discussion -- underlying principles and assumptions:

The USG Cloud Computing Technology Roadmap is a mechanism to define, communicate, and recommend:

- ***Prioritized strategic and tactical requirements that must be met for USG agencies to further cloud adoption;***
- ***Interoperability, portability and security standards, guidelines, and technology that need to be in place to satisfy these requirements; and,***
- ***Candidate Priority Action Plans (PAPs) which are recommended for voluntary self-tasking by the cloud computing stakeholder community to support standards, guidelines, and technology development.***

Following this executive summary, Volume I intentionally presents each requirement at a very basic level, and uses illustrative examples to explain in plain language why from at least one perspective these requirements are not considered to be fully met.

The intent is to lay the groundwork to more directly tackle a subset of cloud computing technology scope, consistent with the Federal Cloud Computing Strategy to accelerate USG cloud adoption. This does not imply an intent to prescribe a USG-centric view.

On the contrary, the "roadmap" is intended to foster a substantive discussion among cloud computing stakeholders in government and the private sector. In practical terms, the roadmap is a vehicle for NIST to fulfill its collaboration role and leverage input from the hundreds of organizations and individuals who have contributed to the NIST-led cloud computing working group analysis and discussions.

Many of the requirements identified in the roadmap are intuitive and common for the adoption of any emerging technology. Throughout the November 2010 – July 2011 time frame, NIST sought to verify the set that are highest priority for USG agencies. The expectation is that while much of the roadmap content will confirm generally accepted priorities, these will also be alternate views. Ideally, responses to the roadmap will refine the requirements and identify relevant work which is under way.

Finally, the roadmap initiative is designed to help ensure that NIST' technical standards, guidance, and research work is focused on the priorities that are most important, not only in the view of NIST computer scientists and researchers, but also in the eyes of those who are building and deploying cloud technology.

The basis for the following list of prioritized requirements is the work completed November 2010 through July 2011 as part of the NIST Cloud Computing program and collaborative effort to develop a *USG Cloud Computing Technology Roadmap*.

The supporting work is summarized in Volume II of the roadmap document which: 1) describes a conceptual Cloud Computing Reference Architecture and Taxonomy, 2) presents USG Business Use Cases and technical cloud use cases, 3) identifies existing applicable interoperability, portability, and security standards and guidance, 4) specifies high-priority standards, guidance, and technology gaps, and

5) provides insight into the rationale for the list of action plans which are recommended for voluntary self-tasking by government and private sector organizations.

The USG Cloud Computing Technology Roadmap requirements which are identified as high priorities to further USG Cloud Computing Technology Adoption are:

Requirement 1: *International voluntary consensus-based interoperability, portability, and security standards (interoperability, portability, and security standards)*

Requirement 2: *Solutions for high-priority Security Requirements (security technology)*

Requirement 3: *Technical specifications to enable development of consistent, high-quality Service-Level Agreements (interoperability, portability, and security standards and guidance)*

Requirement 4: *Clearly and consistently categorized cloud services (interoperability and portability guidance and technology)*

Requirement 5: *Frameworks to support seamless implementation of federated community cloud environments (interoperability and portability guidance and technology)*

Requirement 6: *Technical security solutions which are de-coupled from organizational policy decisions (security guidance, standards, and technology)*

Requirement 7: *Defined unique government regulatory requirements, technology gaps, and solutions (interoperability, portability, and security technology)*

Requirement 8: *Collaborative parallel strategic "future cloud" development initiatives (interoperability, portability, and security technology)*

Requirement 9: *Defined and implemented reliability design goals (interoperability, portability, and security technology)*

Requirement 10: *Defined and implemented cloud service metrics (interoperability and portability standards)*

The content of this document has leveraged an open public process that engaged the broad spectrum of Cloud Computing stakeholder communities and the general public. Input to date has been provided through three public workshops, in May and November 2010, and April 2011, in which more than 1,500 individuals representing hundreds of organizations participated. NIST also consulted with stakeholders through extensive outreach efforts, including, five public working groups formed in November 2010, and the *Federal Cloud Computing Standards and Technology Working Group*. The latter body was formed under the auspices of the US Federal CIO Council to represent common US government interests. This report is subject to a 30-day public review and comment period. All comments received will be considered during the preparation of the final version of this report.

1 Purpose and Scope

1.1 USG Cloud Computing Technology Roadmap Purpose

The collaborative NIST initiative to develop a *USG Cloud Computing Technology Roadmap* and the resulting multivolume interagency NIST DRAFT SP 500-293 document is designed to:

- Foster adoption of cloud computing by federal agencies and support the private sector;
- Reduce uncertainty by improving the information available to decision makers; and,
- Facilitate the further development of the cloud computing model.

This document is intended to serve as:

- A vehicle to define and communicate high-priority strategic and tactical security, interoperability, and portability requirements; these must be met for USG agencies to further adopt the cloud computing model to meet the *Federal Cloud Computing Strategy* goals;
- A vehicle to define and communicate the relevant standards, guidance, and technology that must be in place to satisfy these requirements;
- A vehicle to define and communicate a list of candidate Priority Action Plans (PAPs) to be developed to support security, interoperability, and portability standards, guidance, and technology requirements;
- The mechanism to integrate and present analysis, findings, and useful technical artifacts generated through the NIST Cloud Computing program public working groups, internal NIST Cloud Computing and related projects, and the NIST chaired *Federal Cloud Computing Standards and Technology Working Group*, along with referenced related and complementary work that was reviewed and considered in the roadmap generation process;
- The mechanism to focus discussion on the proposed "technology roadmap" steps to move federal IT from its current early-cloud state ("point A") to a cloud-based foundation ("point B") and to fully execute the US *Federal Cloud Computing Strategy*); and
- The basis to assess and plan the NIST Cloud Computing program and the *Federal Cloud Computing Standards and Technology Working Group* efforts going forward.

1.2 Intended Audience and Use

This publication is intended for a diverse audience:

- **US Policy Makers, US Federal CIO Council, and those with key roles identified in the Federal Cloud Computing Strategy** – as a technology-oriented reference to inform policy and planning;
- **USG Agencies** – as a tool in the context of the USG *Federal Cloud Computing Strategy* risk-based management "Decision Framework for Cloud Migration"; and
- **Cloud Computing Stakeholders (Academia, Government, Industry, Standards Developing Organizations)** – as a consolidated presentation of USG cloud computing technology perspectives, including a list of candidate Priority Action Plans which are recommended for voluntary self-tasking and which present opportunities to leverage stakeholder efforts to further cloud computing.

1.3 Document Organization

The *US Government Cloud Computing Technology Roadmap, Draft Release 1.0 for Public Comment* will evolve and be updated periodically.

The first release of this document consists of two volumes. Consistent with the NIST Cloud Computing program strategy, the roadmap focuses on both strategic and tactical objectives related to cloud computing. The roadmap strategic elements can be characterized as "high-priority technical areas" which are enablers for cloud computing in both the short and long term.

Volume I, *High-Priority Requirements to Further USG Agency Cloud Computing Adoption*, frames the discussion and introduces the roadmap in terms of:

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

Volume I is aimed at interested parties who wish to gain a general understanding and overview of the background, purpose, context, work, results, and next steps of the USG Cloud Computing Technology Roadmap initiative. Volume I reflects the collective inputs of USG agencies through the Federal CIO Council-sponsored *Cloud Computing Standards and Technology Working Group*.

The remainder of Volume I is organized into several sections. Section 2 presents the USG Cloud Computing Technology Roadmap requirements. Section 3 presents other considerations which are related to, but out of the scope of, the roadmap initiative and document. Section 4 identifies the Next Steps, as currently planned for the NIST Cloud Computing program and its collaborative USG Cloud Computing Technology Roadmap initiative.

Volume II, *Useful Information for Cloud Adopters*, is designed to be a technical reference for those actively working on strategic and tactical cloud computing initiatives, including, but not limited to, US government cloud adopters. Volume II integrates and summarizes the work completed to date, and explains how these findings support the roadmap introduced in Volume I.

A third volume, *Technical Considerations for USG Cloud Computing Deployment Decisions,* is under development. Volume III is being developed as an interagency project through the Federal Cloud Computing Standards and Technology Working Group, and will leverage the NIST-led cloud computing program public working group process. Volume III is intended to serve as a guide for decision makers who are planning and implementing cloud computing solutions by explaining how the technical work and resources in Volume II can be applied, consistent with the *Federal Cloud Computing Strategy* "Decision Framework for Cloud Migration." The current version of the working document defines and proposes a methodology and process, and proof-of-concept examples. Volume III was initiated in parallel, but is logically dependent on the technical work contained in Volume II, and will necessarily be completed and presented as part of the roadmap special publication in a subsequent release.

All of these documents are publically available through the NIST ITL Cloud Computing Web site, as are all of the NIST Cloud Computing special publications and work-in-progress documents. See http://www.nist.gov/itl/cloud/index.cfm.

2 USG Cloud Computing Technology Roadmap Requirements

The requirements discussed in this section of the USG Cloud Computing Technology Roadmap are those which have been identified as high-priority strategic and tactical security, interoperability, and portability requirements that must be met for USG agencies to further adopt the cloud computing model to meet the objectives of the *Federal Cloud Computing Strategy*.

Throughout the November 2010 – July 2011 time frame, the NIST Cloud Computing program has sought to analyze, assess, and verify the set of requirements that are of highest priority for USG agencies.

The analysis, assessment, and verification took several forms. This included the public academic, government, industry, and standards developing organization collaborative public working group and outreach activities described earlier. The analysis, assessment, and verification also included the objective, technical research and development activities, internal and collaborative, that are described and referenced in Volume II: *Useful Information for Cloud Adopters*.

Confirmation also included a 60-day parallel review exercise through the *Federal Cloud Computing Standards and Technology Working Group*. The latter includes representatives from approximately 30 U.S. government agencies and focused heavily on the list of USG Cloud Computing Technology Roadmap requirements. This was essential to ensure that the priorities reflect the viewpoint of those in the government who are directly responsible for ensuring that Information Technology resources are applied effectively and securely to support USG agency missions.

There link between:

- Prioritized strategic and tactical requirements that must be met for USG agencies to further cloud adoption;
- Interoperability, portability, and security standards, guidelines, and technology to satisfy these requirements; and
- Recommended voluntary self-tasking Priority Action Plans (PAPs)

is designed to ensure that NIST technical standards, guidance, and research work is focused on the priorities that are important to those who are deploying cloud technology.

Volume I of the technology roadmap intentionally presents the information related to each requirement at a very high level, and uses the illustrative examples to explain in plain language why these requirements are not fully met at present.

The order in which the requirements are listed does not imply relative importance.

2.1 Requirement 1: International Voluntary Consensus-Based Interoperability, Portability & Security Standards

Government, industry, and other stakeholders need to define requirements, develop international voluntary consensus-based interoperability, portability and security standards, and implement them in products, processes and services. (interoperability, portability, and security standards)

Why: *Standards-based products, processes, and services are essential for USG agencies to ensure that: a) potentially large, public investments do not become prematurely technologically obsolete, b) government agencies are able to easily change cloud service providers that can support their missions most cost-effectively and flexibly, and c) the US government is supporting a level economic playing field for service providers.*

Illustrative example of why this requirement is not considered to be fully met at present: *While data, software, and infrastructure components that enable cloud computing (e.g., virtual machines) can currently be ported from selected providers to other providers, the process requires an interim step of manually moving the data, software, and components to a non-cloud platform and/or conversion from one proprietary format to another.*

Rationale: *The development of standards begins with identifying clear unambiguous requirements. USG agencies have identified mission-related requirements that depend on technical interoperability, portability, and security standards. The NIST public Cloud Computing Standards Roadmap Working Group has inventoried general IT standards that apply to cloud computing, and emerging standards that address requirements unique to underlying technologies that enable cloud computing. This effort has identified only three emerging cloud standards to date, although standards organizations are pursuing others. The findings of the NIST Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC)[4] project provides worked examples showing how key technical use cases can be supported in cloud systems that implement documented and public cloud system specifications. SAJACC found interoperability, portability, and security technical use cases to be tightly coupled, which highlights the need for integrated international consensus-based interoperability, portability, and security standards.*

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Develop an initial set of international consensus-based interoperability, portability, and security standards.	2012-2015
Encourage test tool development to support cloud standards development.	2012-2015
Encourage standards conformity assessment practices through procurement.	2012-2013
Define mutual recognition arrangements to allow test reports to be used widely by providers to compete in global markets.	2012-2014
Develop additional technical use cases focusing on multi-cloud scenarios.	2012-2014

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

2.2 Requirement 2: Solutions for High-Priority Security Requirements[5]

As a general requirement, solutions need to be defined to address specific USG high-priority security requirements.

Why: *There is a need to demonstrate that the required level of protection of federal data can be provided in the cloud environment in order to inspire confidence and trust to a level where security is not perceived to be an impediment to the adoption of cloud computing.*

Illustrative example of why this requirement is not considered to be fully met at present: *While cloud computing security requirements are not unique in their entirety or separate from general IT security requirements, the cloud computing environment presents unique security challenges. The architecture, potential scale, reliance on networking, degree of outsourcing, and shared resource aspects of the cloud computing model make it prudent to reexamine current security controls. Multi-tenancy is an example of an inherent characteristic of the cloud environment which intuitively raises a security concern that one consumer may impact the operations or access data of other tenants running on the same cloud.*

Moreover, while it is generally recognized that there are multiple cloud service and deployment models, these have not been sufficiently explored. In the absence of information, to date the focus has been polarized – largely split between commodity and outward-facing low security impact applications in the context of commercial cloud services, and alternately private cloud implementations. For these, as well as hybrid and community deployment models, additional risk and trade-off analysis is needed for the various software, platform, and infrastructure service models.

Rationale: *Federal decision makers need additional information to make risk-based management decisions in migrating critical services or those which store or process sensitive information. Security concerns need to be documented, understood, and addressed to a degree that security in a cloud is clearly understood and managed.*

The Security Requirements list discussed in Volume II of this document was compiled through public working groups and USG agencies in various forums, including the Federal Cloud Computing Standards and Technology Working Group, Information Security and Identity Management Committee, and Federal Risk and Authorization Management Program, and informed by private sector publications.

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Identify Priority Requirements: Continue to list top security concerns of the federal, state, and local government CIO and program community.	2012-quarterly
Identify existing mitigations related to these requirements and assess the extent to which risk can be mitigated through existing and emerging security controls and guidance, such as roles and responsibility analysis and guidance.	2012-periodically
Identify gaps and modify existing controls and monitoring capabilities to address requirements and reduce risks to acceptable levels.	2012-periodically

[5] "Security Requirements" refers to the list of high-priority USG security requirements which must be met to remove perceived impediments to broader USG cloud computing adoption, as presented in Volume II of this document.

2.3 Requirement 3: Technical Specifications for High-Quality Service-Level Agreements

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 *(interoperability, portability, and security guidance and technology)*

Why: *Cloud SLAs represent a negotiated service contract between two parties that specifies, in measurable terms, what cloud service will be provided to the customer. This requirement must be met to ensure that: a) key elements required for cloud services (warranties, guarantees, performance metrics, etc.) are not left out of the SLA and therefore rendered unenforceable, b) common terms and definitions are used within the SLAs to avoid costly misunderstandings between parties, and c) to create an environment which allows agencies to objectively compare competing services.*

Illustrative example of why this requirement is not considered to be fully met at present: *The concept of reliability is a key cloud computing element addressed by practically every provider's SLAs, but how it is defined, what is being measured, and the associated guarantees vary widely. Customers are faced with evaluating different SLAs with cloud providers defining reliability using different terms (uptime, resilience, or availability), covering different resources (servers, HVAC systems, customer support), covering different time periods (hours, days, years), and using different guarantees (response time versus resolution time). SLA ambiguities leave the customer at risk.*

Rationale*: In the process of creating the Reference Architecture, the NIST public working group identified cloud SLAs as being an important gap that needs clarification (scope) and refinement (structure) in order to be fulfilled. A quick survey of the publicly available cloud SLAs showed that an industry-wide accepted standard SLA form for cloud services does not exist. Disparities in cloud providers' SLAs and high-profile issues related to cloud failures have led some to conclude that public cloud SLAs in their current form are of little value to customers. Government agencies have specific requirements (to address policies such as those related to FISMA) which will require modifications to many SLAs.*

The NIST-led public Cloud Computing USG Target Business Use Case, SAJACC, and Security working groups independently and in parallel identified factors related to this same requirement.

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Develop a controlled and standardized vocabulary of cloud SLA terms and definitions.	2012 – update periodically
Ensure consistency in guidance and policy regarding SLA relevant terms and definitions.	2012 – update periodically
Develop a cloud SLA Taxonomy to ensure the complete specification of key cloud computing elements that need to appear in an SLA.	2012 – update periodically

2.4 Requirement 4: Clear & Consistently Categorized Cloud Services

Industry needs to clearly and consistently categorize cloud services. (interoperability and portability guidance and technology)

Why: *This requirement must be met to ensure that: a) customers will understand the intricacies of different types of cloud services and will be better able to select cloud services suitable to meet their business objectives, b) customers will be able to objectively evaluate, compare, and select between products from cloud vendors, and c) providers will have clear guidance where interoperability and portability must exist within similar categories of cloud services.*

Illustrative example of why this requirement is not considered to be fully met at present: *The NIST cloud computing definition has identified three distinct categories of cloud service models: Software as a Service, Platform as a Service, and Infrastructure as a Service. Currently, consumers must seek to understand cloud services through the customized view presented by each service provider. Moreover, while many vendors seek to establish new categories of service, which would improve their market positioning, it is not clear that any proposed categories are unique and not included in the existing three primary services. Examples of proposed additions include Data as a Service, Network as a Service, Service as a Service, and more. The result is a confusing landscape of possible cloud services.*

Rationale: *In late 2010, the NIST cloud computing reference architecture project team surveyed 11 existing cloud computing reference models and services proposed by cloud organizations, vendors, and federal agencies to see if there was any clear industry consensus. Analysis showed a wide disparity. A neutral common understanding and model is needed by customers in order to clearly and consistently understand how cloud services compare (i.e., apples to apples.) In November 2010, the NIST-hosted public working group started with the surveyed reference architectures and explored all proposed recommendations. The group synthesized and leveraged this work through consensus to define a single neutral reference architecture. The initial reference architecture and taxonomy focus on the "what" as opposed to the "how" of implementation, and are not tied to a specific vendor implementation. Although industry participants have validated the model by mapping it to their cloud services, to be useful to USG and other consumers, broader stakeholder validation and participation is needed.*

Recommended Priority Action Plans ***(candidates for voluntary self-tasking by cloud computing community stakeholders)***	Proposed Target Date
Encourage adoption of the NIST Reference Architecture by ISO/IEC JTC1, or an alternate neutral reference architecture through an international consensus-based standards body.	2012 – 2013
Categorize products using the NIST Reference Architecture[6] to provide a consistent view of cloud services to USG agencies.	2012 – update periodically
Encourage suppliers to categorize services consistently.	2012

[6] NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture

2.5 Requirement 5: Frameworks to Support Federated Community Clouds

Industry and the USG need to develop frameworks to support seamless implementation of federated community cloud environments. (interoperability and portability guidance and technology)

Why: *In a Community Cloud deployment, infrastructure is shared by several organizations that have common interests (e.g., mission, security requirements, and policy). In the case where a Community Cloud deployment model is not implemented in one (private cloud or public) environment which accommodates the entire community of interest, there is a need to clearly define and implement mechanisms to support the governance and processes which enable federation and interoperability between different cloud service provider environments to form a general or mission-specific federated Community Cloud.*

Illustrated Example of why this requirement is not considered to be fully met at present: *In the case of a Community Cloud deployed by a single Cloud Provider, the cloud PaaS layer can be used by developers to create applications. As long as the developers establish common technical policies and credentials within that Community Cloud, they can use tools and management systems from different vendors, and connect parts of one application to parts of another application using common PaaS facilities. However, in a federated multi-cloud environment with diverse cloud implementations and policies, the modules may need manual intervention to function together. Technical policies, credentials, namespaces, and trust infrastructure must be harmonized to support a Community Cloud that spans multiple service providers' physical environments.*

Rationale*: The importance of the Community cloud was clearly identified in the NIST-hosted Reference Architecture public working group. The architecture anticipated potential multi-cloud configurations such as Hybrid cloud or those topologies involving a Cloud Broker. It did not address the generalized notion of a federated Cloud Community. USG agencies, the National Security Telecommunications Advisory Committee, and the Open Grid Forum are examples of potential cloud adopters which have identified this as a high priority. The concept has been developed in earlier IT models such as the "GRID," where public and private sector research labs and universities make up a community of High-Performance Computing scientists. Federation techniques have been applied across GRIDs, data centers, and countries to create a "multi-GRID community logical GRID."*

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Define federated Community cloud requirements and scenarios.	2012 – 2014
Identify how Hybrid Cloud and Cloud Broker elements described in the cloud Reference Architecture can be leveraged and harmonized.	2012 – 2013
Present analysis of GRID communities' applicability to federated cloud communities, including technology, trust infrastructure, & governance.	2012 - 2013
All stakeholders -- assess Intercloud efforts (e.g., Standards Developing Organizations) for applicability.	2012 - 2013

2.6 Requirement 6: Technical Security Solutions De-coupled from Organization Policy

Industry needs to define and develop technical security solutions which support, but are abstracted from (and therefore separate from), the decisions required by diverse sovereign, legal, business, or other authoritative policy rules. *(security standards and technology)* Consumers need to adopt consensus technical standards to interoperate with diverse policy rules and authorities. *(security guidance)*

Why: *In the absence of mechanisms to allow differing policies to coexist side by side in a global environment irrespective of geographical location and sovereignty, large-scale interoperability and portability for cloud workloads may not be feasible. Additionally, the ability to bridge policy differences is essential for maintaining service while policies evolve. Security requirements and their associated technical controls, which are essential to ensuring privacy rights and global Ecommerce, will not be universally adopted if they are prescriptively tied to sovereign privacy and security decisions.*

Illustrative example of why this requirement is not considered to be fully met at present: *International government representatives to the World Economic Forum Cloud Computing workshop held in November 2010 identified cases in point – for example, that where one nation considers birth records to be public, and another considers birth records to be subject to strict privacy control. In an EU-US Cloud Computing Technical Seminar, July 2011, representatives discussed the need to support differing EU members' privacy requirements. The TechAmerica Foundation issued recommendations in July 2011 that called for a "technology-neutral privacy framework…,""Security and Assurance Frameworks… which are international..." and "…U.S. government …willingness to trust cloud computing environments in other countries for appropriate government workloads."*

Rationale: *The work of the public and federal security working groups supports the conclusion that the security requirements mentioned in Section 2.2 and discussed in Volume II of this document need to be addressed, and that the development of technical security standards and controls need to take place more quickly than policy consensus. De-coupling the technical implementation of prerequisite cloud security controls from the policy of their application will create an environment that favors cloud computing progress because industry and consumers will be able to agree on an abstract level of security controls, without having to agree on when it is appropriate to apply them.*

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Develop neutral cloud security profiles, technical security attributes, and a test criteria that addresses the USG cloud "security requirements" list.	2012 – 2014
Define an international standards-based conformity assessment system approach.	2013 - 2014

2.7 Requirement 7: Defined Unique Government Requirements and Solutions

Why: *In addition to policy related to cloud services adoption, USG agencies are subject to policy and regulatory requirements, which are unique to government agencies. Government agencies must ensure that cloud services and products meet these policy and compliance requirements as well as mission functionality. Although agencies use commercial services to complete key elements of their mission, USG agencies cannot delegate inherently governmental federal authorities and public trust responsibilities to the private sector. USG institutions cannot mitigate risk through commercial means (e.g., financial penalties, insurance, litigation) to the same degree as private sector organizations. Failure to recognize and address government constraints may slow the adoption of cloud services.*

Illustrative example of why this requirement is not considered to be fully met at present: *OMB memo M-11-11[7] reaffirmed the importance of the implementation of Homeland Security Presidential Directive (HSPD)-12[8] and the need to move quickly to an authentication and access control mechanism which is defined and used government wide. USG agency systems that are not "national security systems" as defined by 44 U.S.C 3542(b)(2) should be required to use Personal Identification Verification (PIV) cards as a way of authentication.[9] This is an example of a requirement where it is necessary to identify and address technology gaps in order for USG agencies to authorize use of cloud services.*

Rationale: *Target USG Business Use Cases have identified cases where government requirement constraints can affect the way the services are designed and implemented and introduce the need for additional features. To expand USG use of cloud computing services, it is necessary to explicitly and objectively identify requirements not currently met in commercial cloud technologies and services, and to formulate strategies to supply missing functionality.*

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Identify regulatory factors that could affect cloud requirements, those which if unmet will prevent adoption by USG agencies, and cloud-based system features that satisfy these regulatory requirements.	2012 – ongoing
Develop technology and products to fill the gaps.	2012 – ongoing

[7] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
[8] http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm
[9] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

2.8 Requirement 8: Collaborative Parallel "future cloud" Development Initiatives

Academia, industry, and USG need to initiate parallel "future cloud" development initiatives. (interoperability, portability, and scalability technology)

Why: *To date, innovation and technology for deploying Web-scale (nation-scale) clouds has been developed by industry. Much of the construction know-how is therefore not available in the public domain; the technology is considered to be intellectual property. USG agencies have legislated, and public trust authorities and responsibilities that cannot be outsourced to private companies, including but not limited to, responsibilities for ensuring that moderate and high security impact systems and data are protected, and that emergency and critical infrastructure public services are provided on a massive scale.[10] Development of a demonstrable and practical technology knowledge base focused on state-of-the-art, nation-size clouds which are scalable and capable, and development of accessible standards and technologies, is needed to solve these nation-scale challenges. A defined baseline of interconnected cloud systems would support additional research and more rapidly lead to world-class cloud advancements that can effectively and securely support critical national priorities and citizen services.*

Illustrative example of why this requirement is not considered to be fully met at present: *Cloud construction and operation, where the number of servers can exceed 100,000 spanning multiple data centers, pose challenges in network design not found in smaller clouds. For example, classic L2 switching (bridging) algorithms, such as spanning trees, do not function at this scale. New L2 techniques which allow for network virtualization are used. Use of L3 (routing) network partitioning techniques introduces routing delays in the middle of distributed caches, streams, or storage pools. Unavoidable speed-of-light delays across geographic distances yield high latency on high-bandwidth links connecting logically joined data centers, making Transmission Control Protocol TCP inefficient. This requirement will create standards and technologies solving these nation-scale challenges.*

Rationale:

Definition of USG target business use cases identified examples where cloud service providers could provide scale to support applications that would benefit the public, and USG agencies could not as cost-effectively or feasibly scale to support the requirement. For example, USG agencies see a need to provide more national geospatial data for public use in emergencies, and cannot outsource their mission in its entirety. A real-life proof-of-concept precedent has been established through Japan's response to the earthquake and tsunami that struck the Greater Tohoku region in March 2011.1[11]

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Define scenarios to support testing of state-of-the-art, interoperable, nation-size clouds.	2012 – 2016
Define project concepts. Identify likely technical and standards challenges.	2012 – 2017
Define conceptual research strategy.	2013 - 2015

[10] N.b. relates to 2011 Cloud Computing analysis in-progress by the National Security Telecommunications Advisory Committee (NSTAC).

[11] *Responding to the Greater Tohoku Disaster, The Role of the Internet and Cloud Computing in Economic Recovery and Renewal*, Internet Economy Task Force, 2011.

2.9 Requirement 9: Defined & Implemented Reliability Design Goals

Industry needs to define and implement reliability design goals, best practices, and related measurement and reporting processes. *(interoperability, portability, and security technology)*

Why: *As USG agencies increase their use of cloud computing to provide essential public services, it is essential that industry be able to ensure that design flaws do not result in catastrophic failures or significant outages over large regions or for extended periods of time.*

Illustrative examples of why this requirement is not considered to be fully met at present: *Cloud Builders create mechanisms to compensate for component failures and deliver High Availability, but the news has highlighted major cloud provider outages. In several cases, cloud providers suffered failures or design flaws which affected the accessibility of cloud-based services for many subscribers. In April 2011, an erroneous network reconfiguration triggered a failure, followed by a cascade of recovery events and subsequent failures, and a lengthy outage. In May 2011, a sequence of cloud outages and software errors led to email delays. During June and July 2011, the same cloud provider suffered outages that disabled services. In August 2011, an intense lightning storm overloaded a power transformer; cloud services were unavailable for hours. In August 2011, a cleanup software bug resulted in customers losing backup data.*

Rationale: *Cloud Computing exemplifies reliability scenarios that are not found in traditional computing and communications architectures. In traditional computing architectures, there is an affinity between the application and the specific hardware on which it runs; high-availability strategies are implemented per-platform, usually through hardware redundancy. In cloud computing, the application and the hardware have less affinity because of virtualization. The economics of hardware redundancy are different in cloud environments in that redundancy within a cloud must be supported by a cloud provider (because users cannot reliably know workload-hardware bindings), and cross-cloud redundancy can trigger additional usage fees. Due to scale, a statistically rare failure event may be a common occurrence in a cloud; clouds compensate with redundancy implemented by cloud software.*

Working with industry and academia, government researchers have identified needs to model, understand, and predict global behavior and ensure reliability in large distributed systems, such as the Internet and computational grids. USG researchers[12] *uncovered design flaws in open-source cloud software that could result in significant resource leakage when systems operating that software are exposed to simple malicious attacks.*

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Formulate and publish best practices on achieving reliability.	2012 – 2014
Develop a consensus process to measure and report industry-wide cloud reliability information to assess current and future cloud reliability.	2012 – 2017
Define research methods for real-time measurement and monitoring to predict onset of catastrophic failure in cloud systems, and tools to identify failure vulnerabilities.	2012 - 2015

[12] C. Dabrowski and K. Mills, *VM Leakage and Orphan Control in Open-Source Clouds.*

2.10 Requirement 10: Defined & implemented Cloud Service Metrics

Industry needs to establish Cloud Service Metrics, including Standardized Units of Measurement for Cloud Resources. (interoperability standards)

***Why**: In utility industries, the notion of units of measurement is fundamental to buying and selling service. Benchmarking is used in traditional computing system operations to determine the performance of system infrastructure such as hardware and operating systems, and for key application platform elements such as database servers and Web servers. However, in the case of cloud computing service delivery, which uses a utility model, IT resources are supplied as abstracted services, often characterized as Infrastructure as a Service or Platform as a Service. For example, networking and storage are often provided as abstracted services. Abstracted services can be set to run fast or slow, to be small or large, and to be as reliable as desired (subject to underlying technology constraints). Service consumers pay for a "quantity" and a "quality" of the service, which is metered by a cloud computing system. Consumers need to be able to precisely specify and receive services.*

***Illustrative example of why this requirement is not fully met at present:** In contrast to the precision with which we categorize units of measurement in electricity, light, or fuels, cloud computing measurements are relatively imprecise. Furthermore, there is no common collection of vendor agreed-upon specific terms. For example, while one provider uses an informal "Elastic Compute Unit," it is imprecise and does not account for workload mix or speed to memory. The characteristics of storage and access to storage over a network vary. Service providers have not defined and applied standardized units of measurement that can be specified in Service-Level Agreements and interoperability exchanges. Therefore, consumers cannot determine and request cloud services as a utility with a high degree of predictability, and cannot achieve maximum cost-effectiveness in cloud computing service application.*

***Rationale**: The USG Target Business Use Case, Reference Architecture, and the public security working groups have all identified this requirement. IaaS services include processing, memory, network, and storage. Considering only storage, for example, a Gigabyte is not the only unit of measurement. There are several "flavors" of storage services: structured and unstructured, replicated and non-replicated, fast-access and slow-access. Furthermore, IaaS attributes have additional dimensionality, such as variation in access speed or processor speed. In other utility industries, the notion of units of measurement is fundamental to creating an economy. This requirement will yield a portfolio of formal Standards for units of measurement in cloud computing, which will be used in a number of ways, from SLA specifications to interoperability exchanges.*

Recommended Priority Action Plans (candidates for voluntary self-tasking by cloud computing community stakeholders)	***Proposed Target Date***
Specify and Standardize the Units of Measurement for cloud services, seeking public comment and collaboration.	2012 – 2013
In parallel, incorporate Cloud Service Units of Measurement consistently in Service-Level Agreements.	2012 - 2013

3 Other Considerations and Observations

The following is a small subset of subjects with which the scope of cloud computing has a Venn diagram-like relationship. Cloud computing is not a subset or a superset of these topics. More specifically, while these topics inform the NIST collaborative initiative to build a *USG Cloud Computing Technology Roadmap*, in their entirety they are outside of the scope of this effort. The topics are listed here to make the point that work in these areas is recognized as being highly interdependent with and essential for overall effectiveness of the roadmap effort.

3.1 Regarding Academia, Industry, Standards Organizations, and Government Collaboration

While there are a large number of cloud community stakeholders accomplishing valuable work in advancing cloud computing standards, guidance, and technology, the rapid pace of cloud computing evolution (which has been characterized as "building the plane while we are flying it") is such that the community needs to work even harder to explicitly leverage our efforts and get ahead of the curve.

For example, there are many approaches to cloud computing standards. In some cases, standards are being developed in consensus-driven working groups, but are not being applied in implementations. In other cases, nonstandardized implementations evolve in parallel, but do not transition to the point where the work is leveraged through formal Standards Developing Organizations. One example of a general benefit that would ensue from aggressively pursuing cloud computing standards is that US government agencies procuring services would be positioned to specify standards, as opposed to specific cloud provider services or products. This would improve cost-effectiveness for the taxpayer and level the playing field for the private sector consumers and service providers.

Collaboration is a productive, but unstructured process that is often driven from the bottom up in the sense that developers and adopters have individual mission, schedule, and resource objectives and constraints. Despite these differences, it is clear that there is much convergence in principle. International technical exchanges[13] and reports[14] illustrate this point. Priorities defined explicitly through recent international conferences hosted by the European Commission and standards organizations,[15] but not exclusively there, include: standards, a level playing field that supports technical innovation, interoperability and open interfaces, a desire to harness the power of cloud to improve public services, a need for improved understanding of cloud computing by policy makers, guidance to architects and engineers, and conformity assessments and testing. An example of a practical collaboration is a mapping exercise that was completed by the EC Standards and Interoperability for Einfrastructure ImplemeNtation InitiAtive (sienna) project to look for commonality and synergism between the NIST technical use cases and Cloud Usage Scenarios with European eScience developments.[16]

---

[13] U.S.-Japan Economic Harmonization Initiative, ICT –IPR Working Group, Washington, D.C., July 2011.

[14] *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology Driven Transformation*, World Economic Forum, 2010.

[15] Ref. ETSI and EC DG INFSO, EuroCIO and EuroCloud, Sophia-Antipolis, France, September 2011.

[16] OASIS International Cloud Symposium, October 2011.

3.2 Interdependency with Cyber Security initiatives

As mentioned in Section 2.2, while cloud computing security requirements are not unique in their entirety or separate from general IT security requirements, the cloud computing environment presents certain unique security challenges resulting from the cloud's very high degree of outsourcing, dependence on networks, sharing (multi-tenancy), and scale. Several initiatives that relate to these challenges are:

The Department of Homeland Security Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) project, which is providing an architecture for dynamic system monitoring and reporting;

The Security Content Automation Protocol (SCAP) initiative at NIST, which provides specifications for expressing security configurations and events, event management, and incident handling;

The National Science Foundation Future Internet Architectures initiative which is developing Internet architectures to provide advanced security and reliability in the context of emerging Internet usage patterns; and

The Federal Information Security Management Act (FISMA). In accordance with the Act, Federal Information Processing Standards (FIPS) 200 and NIST Special Publication 800-53 (periodically updated) provide baseline security controls and guidance for federal information systems.

Security requirements are tightly coupled with interoperability and portability, reliability, and maintainability, which also include considerations which are specific to the cloud computing model. One example of general security work that directly relates to security requirements in the cloud environment is the ability to securely migrate virtual machines between dissimilar organizations or hardware/software environments. In other words, such work aims to provide confidence that before a virtual machine is created in a new physical environment, that environment satisfies the technical policy controls specific to the application and data. Other general areas include authentication techniques such as multifactor authentication with tokens, applied cryptography, and software assurance techniques (e.g., testing and analysis) needed to build confidence that logical boundaries implemented in cloud systems are sufficiently strong to provide security.

3.3 Interdependency with Organizational Policy

The perspective presented in this document is that technology can be used to inform organization policy, and can be used to help implement organization policy, but is not one and the same as organization policy. As highlighted in Section 2.6, it is necessary to have technical solutions which allow differing policies to coexist side by side in a global environment irrespective of geographical location and sovereignty. If not, the benefits of large-scale interoperability and portability for cloud workloads will not be realized. Moreover, the ability to bridge policy differences is essential for maintaining service while policies evolve.

This capability of abstracting technical solutions, so they can be used to implement sovereign policy decisions, but are not prescriptively constrained by specific policy decisions, is essential to universal implementation of the security requirements and associated controls which are critical to ensuring privacy rights and global Ecommerce. This same capability is essential in the development of common commercial application terms of Service-Level Agreements, including commonality of pricing unit definitions, customer protective contract terms, liability ownerships, audit rights, exit provisions, and business continuity.

3.4 Interdependency with Other National Priority Initiatives

The Cloud Computing model is clearly an enabler of national priority initiatives such as Health IT and Smart Grid, and is enabled by programs such as National Strategy for Trusted Identities in Cyberspace (NSTIC). There are tremendous win-win opportunities if we can quickly move toward integrated development of consensus-based cloud computing standards.

An intuitive illustrative target case is the application of cloud computing as an enabler to improve health care for veterans. There is great focus on government security requirements, but other government requirements, such as 508[17] compliance, are often overlooked. One of the strengths of the cloud model is the anytime/anywhere deployment on a broad variety of end-devices. This would be a key advantage in addressing disability access. Physical disabilities, post-traumatic stress disorder, or depression can make downloading 508-compliant profiles to individual devices challenging. One way to help address this is to deploy Health IT systems using a common profile that defines a preference specific to each individual. However, the benefit of achieving this scenario applies much more broadly than satisfying a government requirement or supporting a specific interest group. The same solution could be applied to improve the ability of parents, educators, and other responsible parties to screen Internet-accessible content by minors. Over and above these specialized requirements, the same capability could be leveraged to improve convenience and ease of use for all cloud service users. These requirements can be met without applying the cloud model – the cloud computing model is simply an enabler that has the potential to accelerate this capability. This concept intuitively demonstrates the relationship between roadmap requirements and practical implementation. A simple test of the capabilities described above would require integrated security standards to secure the data and protect the privacy of the profile as well as the data, data portability, and interoperability at the software, platform, and infrastructure levels of cloud.

Information security is naturally a critical factor for widespread adoption of Cloud Computing. For government users, particularly early adopters, security fears are front and center. In addition to data confidentiality, integrity, and availability, the need for trusted identities and secure and efficient management of these identities while users' privacy is protected is a key element for the successful adoption of any cloud solution. Augmenting security technologies and best practices, NSTIC will enhance security and privacy for cloud services. NSTIC defines a means to create a secure, trusted *Identity Ecosystem* that is capable of establishing a user-centric privacy protection for any Cloud Ecosystem. It is generally acknowledged that the use of passwords does not provide optimal security or assurance. The NSTIC Strategy[18]calls for the development of interoperable technology standards and policies — the "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The mechanisms employed by an *Identity Ecosystem* are structured in a robust *framework* comprised of the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms. Individuals will be able to validate their identities and then securely access the Identity Ecosystems. Within NSTIC's trusted framework of defined security requirements based on risk and sensitivity, Cloud services will be more securely supported. The objective is more than lowering cost and increasing access; it also supports interoperability, portability, and security.

[17] Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998....REQUIREMENTS FOR FEDERAL DEPARTMENTS AND AGENCIES.-- ... (1) ACCESSIBILITY

[18] http://www.nist.gov/nstic/about-nstic.html

4. Next Steps

This document marks the completion of the first phase of the NIST Cloud Computing program and initiative to collaboratively build a *USG Cloud Computing Technology Roadmap*. This milestone is consistent with the strategy defined in the program planning phase, May through October 2010, and with the program time line presented in November 2010.

As described previously, this roadmap document is a practical mechanism to integrate and present analysis, findings, and useful technical artifacts generated through the NIST Cloud Computing program public and federal working groups, and internal NIST projects.

However, strategically, the roadmap publication also provides an opportunity, as intended, to assess progress and effectiveness. The NIST initial assessment is that the collaborative approach has been effective, and the initiative has met the goal of technically advancing the cloud computing model – particularly in its target area of interoperability, portability, and security standards, guidance, and technology requirements.

NIST bases its initial assessment on the 18-month continued level of engagement with the cloud community in public working groups and NIST Cloud Computing Forum and Workshop events. Hundreds of individuals and organizations are registered working group members, and the NIST-hosted cloud forum events have been registered to capacity. In terms of results, the "useful information for cloud adopters" available publically on the NIST Cloud Computing Web site and special publications produced from NIST projects and working groups are widely referenced and used. These are summarized in Volume II of the roadmap document. The most widely recognized work, after the *NIST Cloud Computing Definition*, SP 800-145(Draft), is the *NIST Cloud Computing Reference Architecture*, SP 500-292, which was issued in September 2011. It is currently being used as the basis for developing a standardized reference architecture by international standards bodies, and by US government agencies and industry for its intended purpose of categorizing cloud services so that government agencies and others can compare cloud services from different providers more easily.

NIST also bases its assessment on the review and support for the *US Government Cloud Computing Technology Roadmap Volume 1, Release 1.0, (DRAFT) High-Priority Requirements to Further USG Agency Cloud Computing Adoption* by the representatives designated by the US Federal CIO Council to participate in the Federal Cloud Computing Standards and Technology Working Group. Confirmation of the priorities presented here by a broad sample of representatives of USG organizations who are responsible for deploying IT to support agency missions reinforces the conclusion that "we" – NIST and its cloud community collaboration partners – "got it right" in terms of the objectives for the effort and the roadmap.

Given this assessment, the following section presents the current thinking, strategy, and plan for the NIST Cloud Computing program and USG Cloud Computing Technology Roadmap initiative to now leverage this initial roadmap going forward, and take our next steps toward the overall goal of supporting USG agencies in the secure and effective deployment of cloud computing.

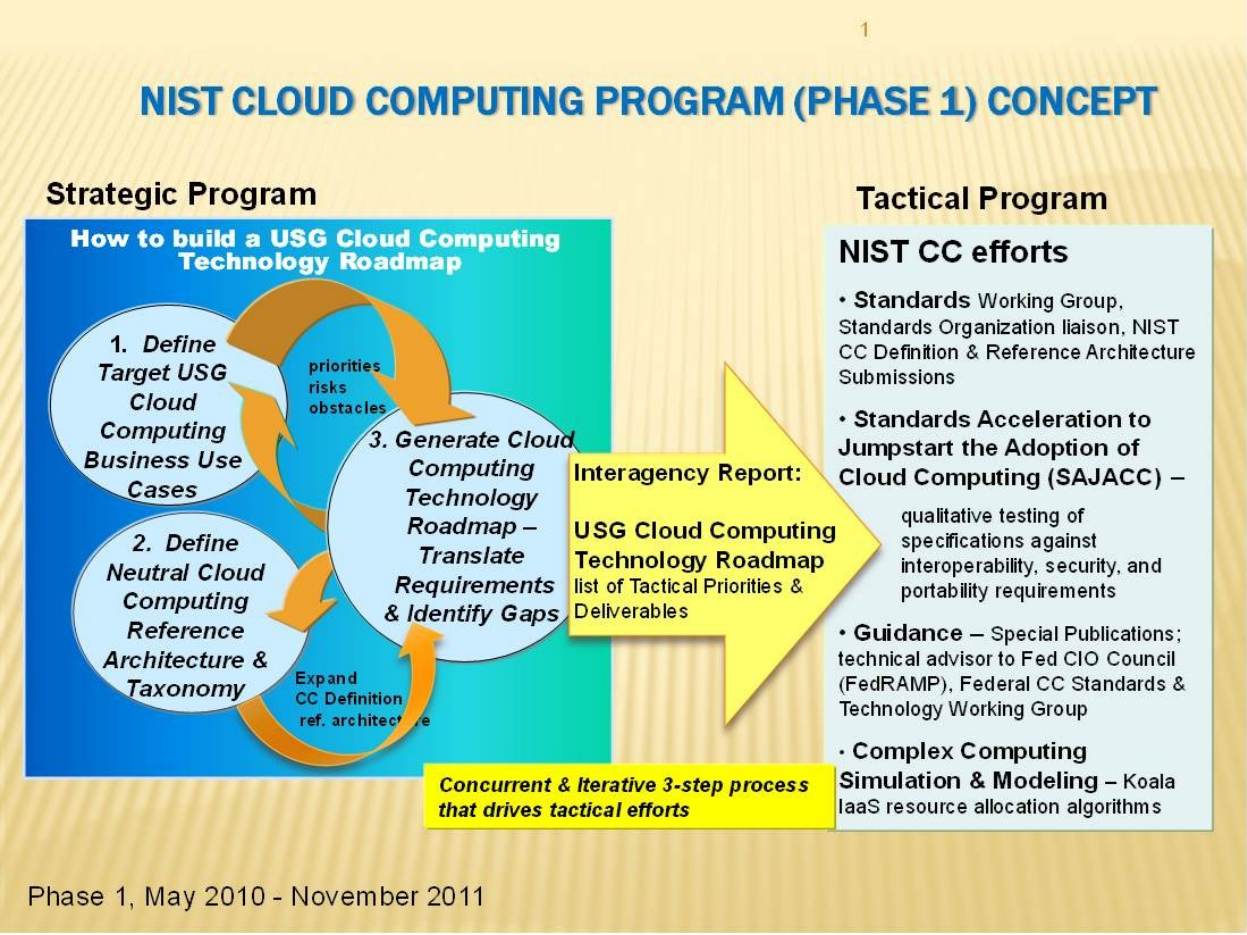
The expectation is that this initial strategy and plan for Phase 2 of the NIST Cloud Computing program and USG Cloud Computing Technology Roadmap initiative will be revised based on the insights and

opinions received during the public comment period, as well as other factors, including but not limited to, US government national program priorities. The target for confirming the strategic scope of the second phase of the NIST Cloud Computing program is the first quarter, calendar 2012. Tactical projects and working groups are planned to continue November through March 2012, as they were initiated in Phase 1, described below.

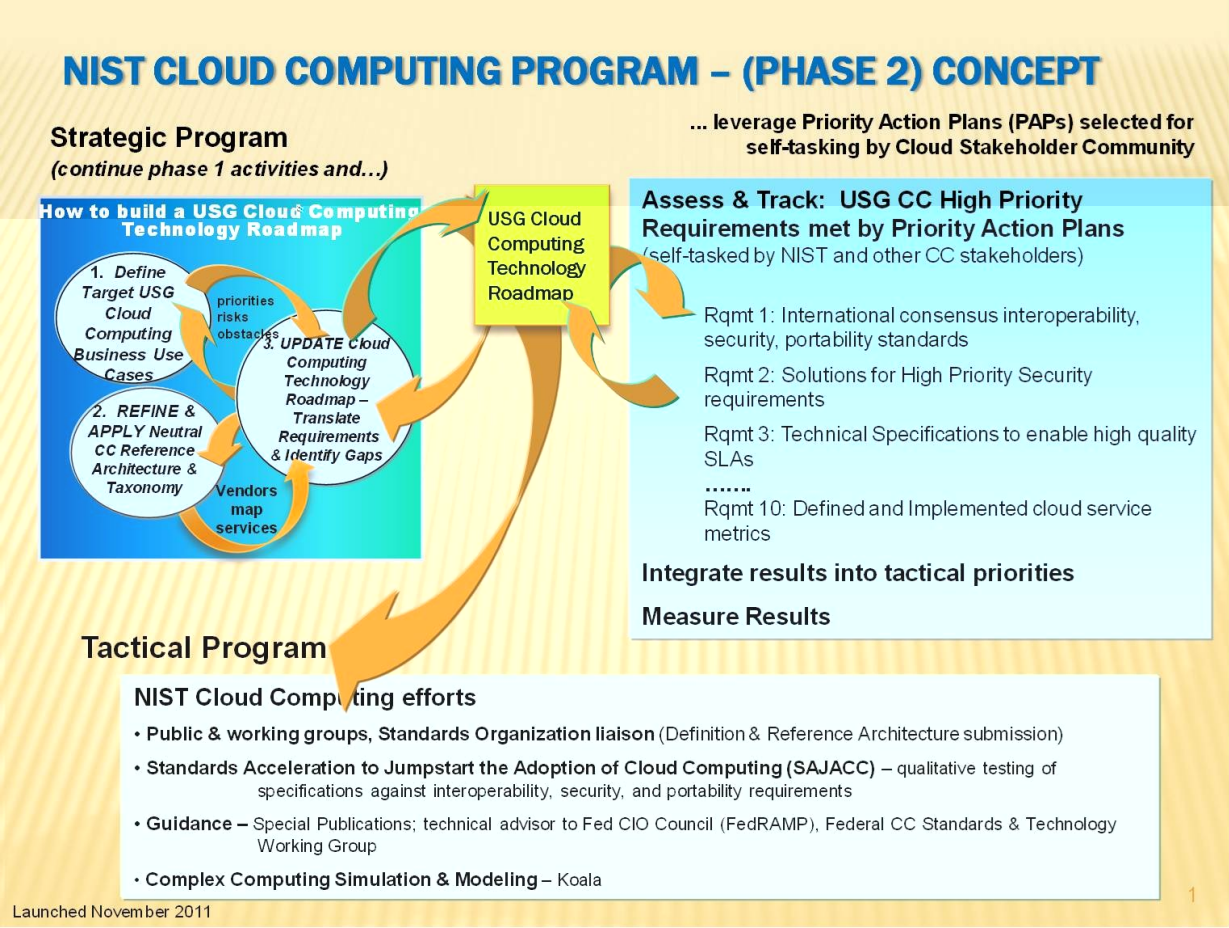
Regardless of the refined assessment and revised strategy for the NIST cloud computing program going forward, the expectation is that the program will continue to produce focused deliverables at measured six-month intervals, continue its presence through outreach activities and interactions with other USG and international stakeholders, and track progress towards the priorities presented in this document.

4.1 NIST Cloud Computing Program Phase II

Phase 1 of the NIST Cloud Computing program effectively established and integrated three strategic processes, public working groups, and NIST cloud efforts to develop the first USG Cloud Computing Technology Roadmap, and help NIST to prioritize its internal projects.



Phase 2 of the NIST Cloud Computing program continues the Phase 1 scope and activities. In addition, Phase 2 introduces new strategic activities to leverage the *USG Cloud Computing Technology Roadmap* produced in Phase 1.

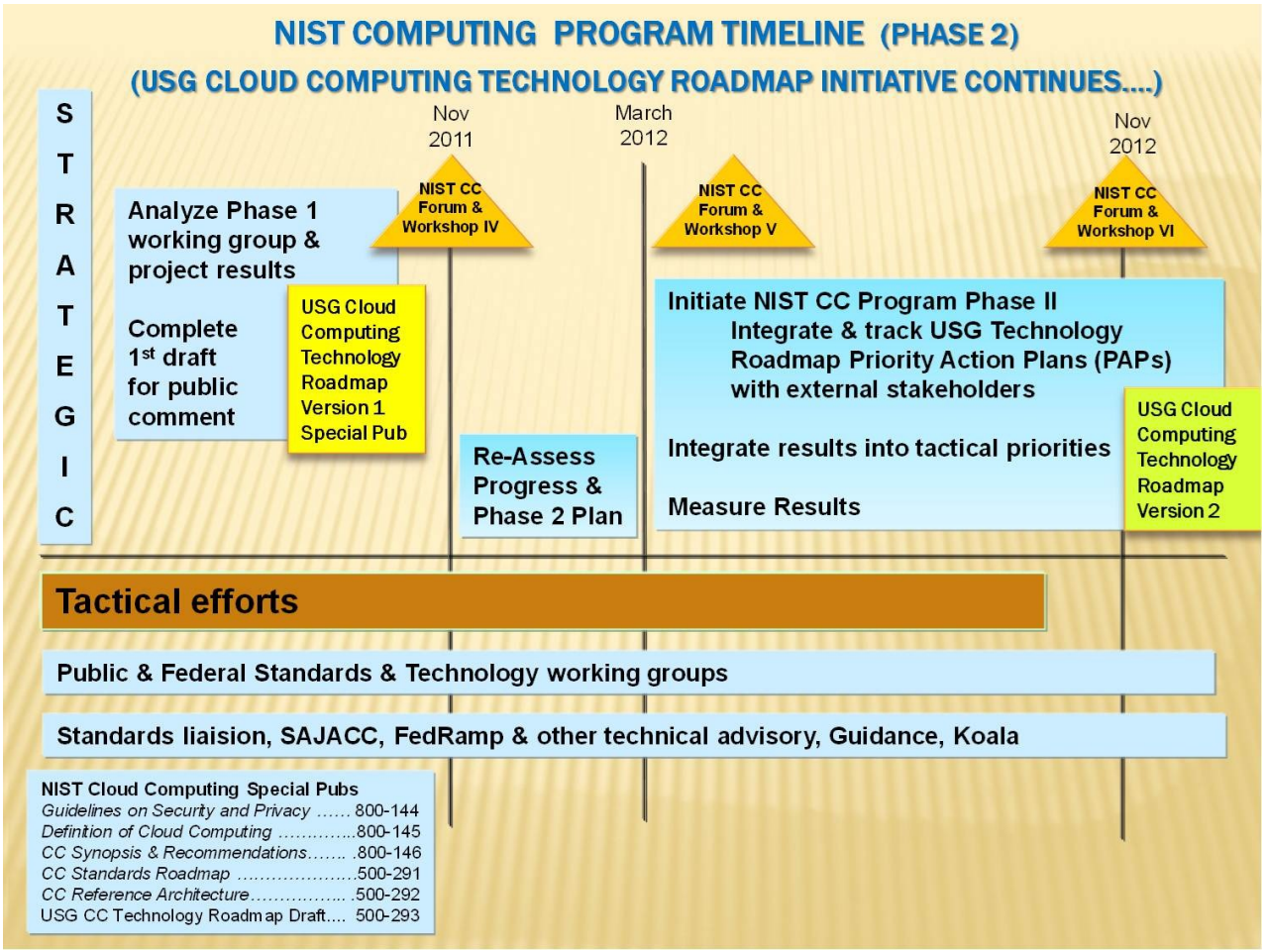


Phase 2 is planned to include:

- Applying the USG Cloud Computing Business Use Case template to develop and make publically available a larger set of USG agency mission use cases;
- Leveraging this effort to complete and issue the roadmap Volume III: *Technical Considerations for USG Cloud Computing Deployment Decisions*;
- Validating the Phase 1 Reference Architecture (SP 500-292) through cloud service provider examples of categorized services, and working with cloud stakeholders to establish a repository of the mapped vendor services to support USG and others in comparing cloud service offerings;
- Continuing to identify high-priority interoperability, portability, and security requirements which must be met for USG agencies to accelerate the adoption of the cloud computing model; continuing to assess standards, guidance, and technology that must be in place to meet these requirements, and recommending Priority Action Plans (PAPs) for voluntary self-tasking by the cloud stakeholder community, to support standards, guidance, and technology advancement;

- Working with cloud stakeholders to identify efforts which satisfy the objectives of the PAPs, assessing and communicating the extent to which the requirements are satisfied, and defining processes to leverage these efforts to support the USG adoption of cloud computing;
- Identifying the subset of PAP objectives which are consistent with NIST core mission standards, guidance and research activities; developing NIST PAP plans, and executing those plans;
- Integrating these strategic activities with NIST tactical program projects and working groups; continuing to deliver special publications, technical guidance, and support collaborative Web-based tools to support these tactical efforts;
- Defining and tracking measures and metrics to assess program effectiveness;
- Continuing outreach activities including the NIST Cloud Computing Forum & Workshop series to calibrate and leverage NIST efforts with the broader stakeholder community; and
- Analyzing and assessing the technical work completed through these efforts, and applying this analysis to revise the *USG Cloud Computing Technology Roadmap* on a periodic basis.

4.2 Time Line and Deliverables



Appendix A: USG Interagency partners and contributors

Bruce Beckwith, Department of Energy

Kathy Conrad, Principal Deputy Associate Administrator, General Services Administration

Earl Crane, Department of Homeland Security, Information Security and Identity Management Committee (ISIMC)

Dominic Gomes, Office of the Chief Information Officer, Department of Health and Human Services

Lon D. Gowen, Ph.D., National Aeronautics and Space Administration (NASA), Goddard Space Flight Center

Audrey M. Hogan, Tennessee Valley Authority

Dr. Prabha N Kumar, Special Assistant, Department of Defense, OCIO

Festus C. Onyegbula, Office of Information Technology, National Institute of Food and Agriculture, U.S. Department of Agriculture

James Ramskill, Office of the Director of National Intelligence

David Raw, Office of the Chief Information Officer (OCIO), Department of Homeland Security

Lew Sanford Jr., DCS-OESAE, Social Security Administration (with other SSA participants)

Charles Santangelo, Senior IT Budget Manager, Capital Planning and Governance, OCIO, Office of the CIO, NASA

Param Soni, Environmental Protection Agency

Gerald L. Smith, Department of Defense and OASIS

Peter Tseronis, Chief Technology Officer, Department of Energy