

Emerging Standards and Initiatives to Support the Adoption of Cloud Computing by the U.S. Government

May 25, 2010

By Jim Graham, Senior Vice President, SecureIT

Overview

There are a number of major developments underway which will radically change the delivery of information technology (IT) services and the manner in which the Federal Government implements IT security. Some of these developments are leveraging emerging trends such as Cloud Computing and Data Center Consolidation. Others get their impetus from the increase of advanced persistent threats, the drive for cost savings, efficiency and increased effectiveness. In either case, these developments affect Federal Government agencies as well as the companies and non-profit organizations which provide services to federal agencies. The purpose of this letter is to provide a perspective on cloud computing initiatives highlighting important aspects which impact planning and implementation of cybersecurity. For each area a brief summary of how these initiatives impact government and commercial organizations is presented.

Examples of Early Adoption

Recent initiatives demonstrate the Federal Government's move to cloud computing. In cases involving procurement of commercial services, compliance with Federal government

security requirements is specified with the objective of getting compliance with FISMA built in. Examples include:

- General Services Administration (GSA) [Infrastructure as a Service \(IaaS\)](#) procurement
- Treasury Capital Planning and Investment Control (CPIC) Cloud Procurement
- [Army Private Cloud \(APC2\)](#)
- National Aeronautics and Space Administration (NASA) [Nebula](#) private cloud services
- Defense Information Systems agency (DISA) [Rapid Access Computing Environment \(RACE\)](#) private cloud services

NIST Cloud Computing Standards

Government, corporations and non-profit organizations are carefully considering the advantages and challenges posed by adoption of cloud computing. Cloud computing capabilities are rapidly evolving and gaining in adoption primarily due to the financial savings. National Institute of Standards and Technology (NIST) has prepared what is generally recognized as the [definition of cloud computing services](#) which is summarized in the figure on the following page.

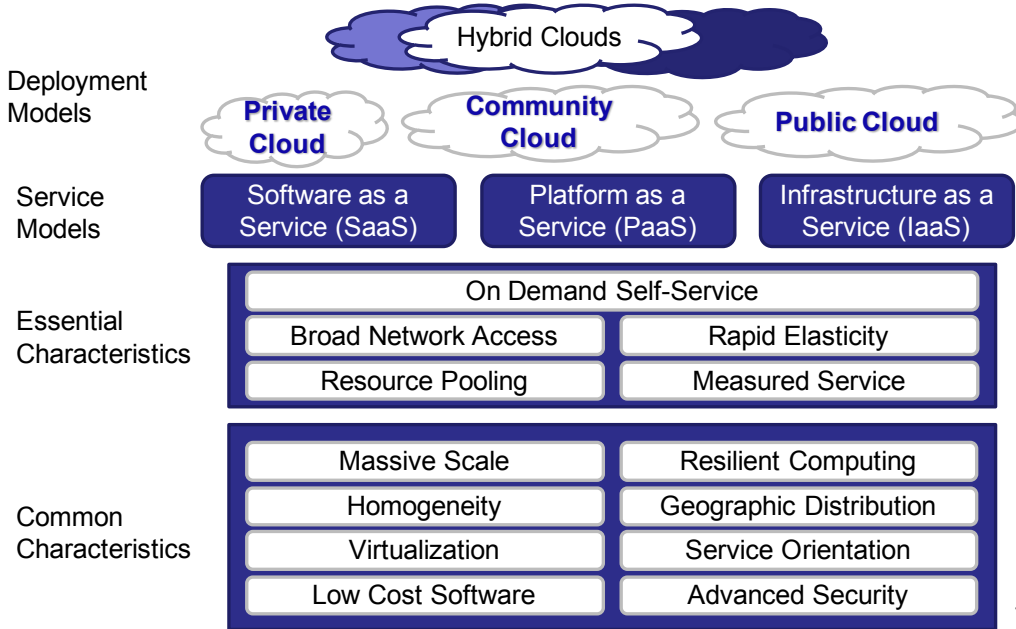
The Federal government has recently communicated a strategy for speeding the adoption of cloud computing solutions described as:

- Shift to a “cloud-first” policy
- Identify opportunities through data center Cloud Computing Framework, courtesy GSA
- Consolidation
- Centralize certification of cloud solutions (FedRAMP)
- Establish standards for security, interoperability & data portability

consolidation efforts, to identify those which could be candidates to benefit from cloud computing (be it private, community/hybrid or public).

Presently, adoption of cloud computing is hampered by IT security challenges which consist of:

- Inability to trust the vendor’s security model
- Customer inability to respond to audit findings
- Multi-tenancy and potential inability to isolate customer data



- Obtaining necessary support for investigations
- Personnel security standards to meet Federal standards
- Indirect administrator accountability
- Proprietary implementations that cannot be examined
- Loss of physical control and inability to limit where data can be stored
- Data portability / ability to transfer to a different provider

15

Cloud Framework and Definition, courtesy Peter Mell, NIST

Federal Cloud Computing Initiative

The vision is to establish a shared government-wide, cost effective, green and sustainable federal cloud computing environment that will support agency missions by enabling secure, easy to use, rapidly provisioned, cloud computing services. GSA has already embarked on its role in executing this mission through the creation of www.Apps.gov and with procurements for Software as a Service (SaaS) and IaaS. The goal of Apps.gov is to provide a solution for federal agencies to locate and purchase cloud-based services. Apps.gov offerings will be populated from GSA Schedule contracts. The Federal CIO is also urging Department and Agency CIOs to examine their portfolios, particularly data center

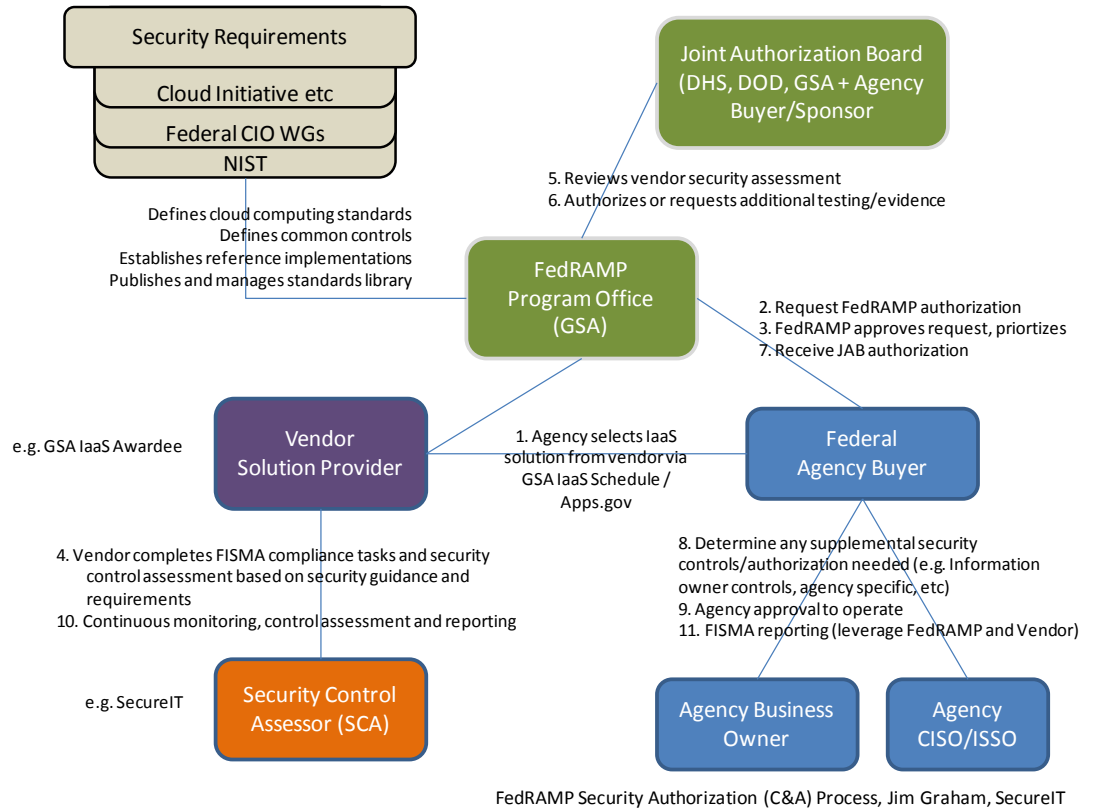
SAJACC and other NIST Standards

NIST is currently developing two Special Publications (SP) to provide guidance on cloud computing implementation by Federal agencies. Expected out later this year, the intent of these publications are to provide agency IT executives with criteria to aid in decision making regarding selection and implementation of cloud computing to benefit their organizations. One SP will provide guidance to aid in cloud computing solution development and use by agencies. It will provide guidance on interoperability, portability, and security. This publication will formalize the current NIST definition of cloud computing and provide informal recommendations. The second publication will provide

guidance on secure usage of virtualization technologies which is a key underlying technology that powers cloud computing. The publication will provide an overview of full virtualization technologies, discuss the security concerns associated with full virtualization for servers, and provide recommendations for addressing them. The publication will also give an overview of actions that organizations should perform throughout the lifecycle of a server virtualization solution.

A second major initiative from NIST is the Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC). The purpose of this initiative is to provide an information sharing and collaborative environment between the Federal Government and industry for the rapid development of cloud computing use cases and associated specifications. Together with the Federal Cloud Computing Initiative, the intent is to accelerate the development of standards while not limiting innovation. As use cases are defined, specifications can be developed and rapidly reviewed and commented on by industry. Reference implementations can be identified to aid in communicating the use case and implementation to conformance with specifications.

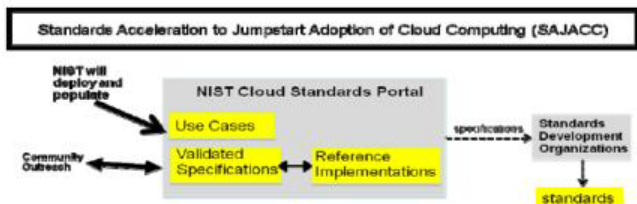
remains to be decided upon. However, in the interim, the SAJACC will provide an invaluable resource to the community and can complement other industry standards efforts such as those at [OASIS "Identity in the Cloud"](#), [DMTF "Open Cloud Standards Incubator"](#) and the [Cloud Security Alliance](#).



FedRAMP Security Authorization (C&A) Process, Jim Graham, SecureIT

FedRAMP

Enter the Federal Risk Authorization and Management Program (FedRAMP). FedRAMP was conceived as a program to address these challenges. It is a Federal government-wide initiative managed by GSA with joint participation from NIST, Office of Management & Budget (OMB), Department of Homeland Security (DHS), and Department of Defense (DOD) to develop a program to unify security requirements and security authorizations for shared services such as those offered by cloud computing. The benefit to government agencies is that users of a FedRAMP authorization service would not need to perform or require separate security testing and authorization. The agency could leverage the authorization provided by the FedRAMP program. Companies that provide cloud computing or other forms of



How NIST will facilitate or harmonize standards development without hampering innovation or picking winners and losers

shared services to the government will be able to obtain an authorization from the FedRAMP program which will meet most federal agency requirements. The diagram above depicts the anticipated process. The GSA IaaS procurement is currently planned to be the first user of this process.

The FedRAMP program office in conjunction with the Security Requirements Authorities are in the process of devising examples for system boundaries for the different cloud computing models at the MODERATE security baseline level. This will enable the determination of control ownership between the cloud provider and the user agency. This guidance will aid agency procurement efforts to more accurately define control ownership as well as indicate where agencies will need to perform supplemental efforts. For example, a SaaS implementation will require significant security control implemented by the cloud computing provider whereas an IaaS implementation will be less control as the agency will have control over deployment of services and applications in the IaaS cloud.

Cloud Security Alliance

The Cloud Security Alliance (CSA) is a non-profit organization formed in 2008 to promote the use of best practices for providing security assurance within Cloud Computing. The association members perform outreach and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is comprised of subject matter experts from a wide variety of disciplines. The objectives of the Cloud Security Alliance are:

- Promote a common level of understanding between the consumers and providers of cloud computing regarding the necessary security requirements and attestation of assurance.
- Promote independent research into best practices for cloud computing security.
- Launch awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions.
- Create consensus lists of issues and guidance for cloud security assurance.

To support these objectives, the Cloud Security Alliance has produced and made available its "[Security Guidance for](#)

[Critical Areas of Focus in Cloud Computing](#)¹" present at version 2.1. The guidance is intended as a process as opposed to a framework. The following steps are provided to aid organizations in evaluating appropriateness and risk tolerance for transition of assets / services to one of the defined cloud computing models. These critical steps include:

- Identify the asset for the cloud deployment
- Evaluate the asset
- Map the asset to potential cloud deployment models
- Evaluate potential cloud service models and providers
- Sketch the potential data flow

Perspectives

Public Sector CIOs and Business Owners

Agency officials need to examine current business processes and IT solutions to identify candidates for cloud computing. Using the guidance from CSA supplemented along with the resources from NIST, SAAJCC and upcoming special publications validate candidates and devise requirements from the base of use cases and specifications that exist today.

If obtaining a cloud computing service which will be used by more than three (3) federal agencies, consider requesting the FedRAMP program to lead security authorization certification & accreditation (C&A). If the cloud computing service/solution has a current C&A, determine its applicability and identify any security requirements over and above that which are defined and were tested. Supplement the C&A with testing for your unique agency requirements.

Service/Solution Providers

Organizations that currently or are planning to offer cloud computing solutions to Federal or State Government agencies need to develop a strategy which aligns with FedRAMP to ensure the appropriate security controls are implemented, controls are independently assessed and the necessary evidence is prepared. When your company sells this service, work with your government customer to determine if your service is appropriate for FedRAMP. Execute your strategy

¹ Copyright © 2009 Cloud Security Alliance

which includes preparing security plans, addressing control gaps and obtaining an independent assessment from a firm such as SecureIT. This will enable your company to provide the necessary evidence to support a review by the Joint Authorization Board. When the authorization is obtained the sponsoring agency may need to perform some supplemental testing prior to authorization. However, with FedRAMP authorization obtained, the vendor can market this to other prospective customers with the benefit of more rapid service delivery.

About the Author



Jim Graham is the Senior Vice President for Federal Programs at SecureIT. He has over 25 years of experience providing IT solutions and IT security professional services to Federal government agencies and commercial businesses. He has held technical and management leadership

positions at McDonald Bradley, LEADS Corporation, DOMAIN Technologies and TRW and is a Certified Information Systems Security Professional (CISSP). Jim is active in industry associations including [ACT/IAC](#) where he is the Vice Chair for Cybersecurity. Jim can be reached at jgraham@secureit.com.

About SecureIT

SecureIT helps private and public sector clients manage technology risks and implement secure and trusted information systems through effective practices in IT security and privacy. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT devises strategies and solutions to address the unique business needs and environments of our clients resulting in reduced risk and increased efficiency. Leveraging our knowledge and experience with industry regulations and standards, we assist our clients to overcome the challenges of compliance with FISMA, FISCAM, HIPAA, HITECH, Privacy Act, SOX, and PCI. Founded in 2001 and located in Reston, VA, SecureIT serves the U.S. Federal Government, Financial Services & Banking, Healthcare, Public, Private and Non-Profit organizations.



1902 Campus Commons Drive, Suite 100
Reston, VA 20191
info@secureit.com
www.secureit.com
703-464-7010

The SecureIT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group. Other company names or products mentioned are or may be trademarks of their respective owners. Information in this document is subject to change without notice.