Anexo III

U.S. FEDERAL STRATEGY FOR THE SAFE AND SECURE ADOPTION OF CLOUD COMPUTING

Bill Perlowitz, Vice President, Advanced Technology, Apptis, Inc.
William.Perlowitz@Apptis.com, http:/ /www.linkedin.com/in/wperlowitz

ABSTRACT

The FDCCI

The reported number of Federal data centers grew from 432 in 1998 to 2,094 in 2010. This growth in redundant infrastructure investments is costly, inefficient, un sustainable, and has a significant impact on energy conswnption. In 2006, Federal servers and data centers conswned over 6 billion kWh of electricity and without a fun damental shift in how the Government deploys technology it could exceed 12 billion kWh by 2011. In addition to the energy impact, information collected from agencies in 2009 shows relatively low utilization rates of current infrastructure and limited reuse of data centers within or across agencies. The cost of operating even a single data center is significant, and includes hardware and software costs, real estate costs, and power and cooling costs.

The Federal Data Center Consolidation Initiative aims to address these challen ges by leveraging the best practices of the public and private sector. The focus of this initiative is to:

Promote the use of green it by reducing the overall energy and real estate foot
Print of government data centers
Reduce the cost of data center hardware, software, and operations
Increase the overall it security posture of the government
Shift it investments to more efficient computing platforms and technologies

The Federal Government has issued FDCCI guidance for Federal CIO Council agencies, calling for them to inventory data center assets, develop consolidation plans throughout fiscal year 2010, and integrate those plans into FY 2012 budget submissions. Through the FDCCI, a minimum of 800 of these data centers will be closed by 2015.

As shown in Figure 1, the Data Center Consolidation Initiative Agency Consolidation Plan Template provides consolidation via one of the four approaches:

Approach	Description	Potential Benefits	Rationale
Decommission	Turn off servers that are not being used or used infrequently (e.g. dedicated development environments)	• Cost Savings • Energy Efficiency • Frees Floor / Rack Space	• As many as 10-15% of servers may be inactive but still powered on in data centers*
Centralization / Site Consolidation	Move servers/storage to a few selected data centers Consolidate small data centers to larger target centers	• Floor Space Cost Savings • Operational Cost Savings • Increase Rack Utilization • Energy Efficiency	• Approximately 430 Government data centers are categorized as 'closets' or small sized data centers (less than 1,000)**
Virtualization	Consolidate several servers onto a single server through virtualization of the OS/Platform	• Floor Space Cost Savings • Increase Rack Utilization • Increase Server Utilization • Energy Efficiency	• Server Utilization is approximately 21% Government wide**
Cloud Computing Alternatives	Move application functions to standard, vendor supported enterprise platforms or services	• Floor Space Cost Savings • Energy Efficiency • Operational Cost Savings • Cap Ex Cost Savings HW/SW • Reduced SW Maintenance • Improved Service Delivery	• Reduce Operational Risk, lower TCO and TCSD • Approximately 60% of Civilian Agency Systems are low-impact FISMA security, and therefore may be low-risk candidates for Cloud Computing solutions

* McKinsey Report: Revolutionizing Data Center Efficiency, July 2008
** OMB EDP 09-01 Data Analysis, October, 2009

The DCCI define and monitors standard operational metrics across Agencies, and achieves efficiency gains and realize operational cost savings by improving:

Server (CPU) Utilization(%)
Rack Space Utilization(%)
Rack Floor Utilization(%)
Power Usage / Square Foot
Power Usage Efficiency (PUE)

As shown in Figure 1, each Federal agency may evaluate cloud computing as one of four options to approach for Data Center Consolidation on an application by-application basis. The resulting consolidation of data centers across the Federal Government will achieve cost savings, reduce energy consumption, optimize space utilization, and improve IT asset utilization.

25 Point implementation plan

The 25 *Point Implementation Plan to Riform Federal Iriformation Technology Management* will be completed by the end of June 2012, and details how the Federal Government will deliver more value to the American taxpayer. The Plan requires a focus on exe cution and is designed to establish early successes to garner momentum for continued efforts.The first six points of the Plan describe the application of "Light Technology" and shared solutions, and focus on consolidating existing data centers, reducing the need for infrastructure growth by implementing a "cloud first" policy for services, and increasing government use of available cloud and shared services.

The Plan stipulates that: Beginning immediately, the Federal Government will Shift to a "cloud first" policy. The three-part strategy on cloud technology revolves around using commercial cloud technologies where feasible, launching private Government clouds, and utilizing regional clouds with state and local governments where appropriate. When evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effec tive cloud option exists. To facilitate this shift, the government will be standing up secure government-wide cloud computing platforms.

To jump-start the migration to cloud technologies, each Agency CIO is required to identify three "must move" services and create a project plan for migrating each of them to cloud solutions and retiring the associated legacy system. Of the three, at least one of the services must fully migrate to a cloud solution by December 2011; with the remaining two migrated by the end of June 2012.

By December 2011, the Federal CI0 will also develop a strategy for shared services. This strategy will build on earlier Federal Government successes in shared ser vices and include benchmarks on current usage and uptake rates, as well as Service Level Agreements (SLAs), customer satisfaction levels, costs, and overall economic effectiveness.

Managing partners of shared services will assess the current state of shared services and will each release a roadmap to improve quality and uptake. Ultimately, the managing partners will be responsible for executing these roadmaps and will be held accountable for improvements in SLAs and reductions in cost. These efforts will enable shared services to be accessible Government-wide at continually higher quality levels.

Federal cloud computing strategy

In FY 2010, approximately thirty cents of every dollar invested in Federal IT was spent on data center infrastructure. Unfortunately, only a fraction of this investment delivers real, measurable impact for American citizens. By using the cloud computing model for IT services, the Government will be able to reduce data center infrastruc ture expenditure by approximately 30%. Similar efficiency improvements will be seen in software applications and end-user support. These savings can be used to increase capacity or be reinvested in agency missions, including citizen-facing services and inventing and deploying new innovations.

The Federal Cloud Computing Strategy ("Strategy") describes how Federal cloud computing holds tremendous potential to deliver public value by increasing opera tional efficiency and responding faster to constituent needs and how applying cloud technologies across the entire Federal Government can yield tremendous benefits in efficiency, agility, and innovation. These benefits are described in Figure 2.

Efficiency improvements will shift resources toward higher-value activities
Assets will be better utilized
Demand aggregation will reduce duplication
Data center consolidation can be accelerated
IT will be simpler and more productive
Agility improvements will make services more responsive
Services will be more scalable
Innovation improvements will rapidly enhance service effectiveness
An entrepreneurial culture will be encouraged by reducing risk

The Strategy details that cloud is a fundamental shift in IT that can significandy improve public sector IT. Specific benefits detailed in the Strategy include:

The Strategy includes a structured framework with a strategic perspective for agencies to consider and plan for cloud migration, and presents a nwnber of activities that Federal Government leadership can undertake to facilitate adoption and mitigate risk. We discuss these in the next section.

The Strategy is also the document that clearly articulates that the policies and plans described in this section are official policy to be acted upon by agencies: "Following the publication of this strategy, each agency will re-evaluate its techno logy sourcing strategy to include consideration and application of cloud compu ting solutions as part of the budget process."

"Consistent with the Cloud First policy, agencies will modify their IT portfolios to fully take advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost."

Figure 2. Federal Cloud Computing Strategy
Benefits: Efficiency, Agility, Innovation

EFFICIENCY	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
AGILITY	
Cloud Benefits	**Current Environment**
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
INNOVATION	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

POLICIES AND PLANS SUMMARY

The Government has recognized a responsibility to achieve the significant cost, agility, and innovation benefits of cloud computing as quickly as possible.

OMB Budget guidance, the Federal Data Center Consolidation Initiative, the 25 Point Implementation Plan to Riform Federal IriforrnatWn Technology Management, and the Federal Cloud Computing Strategy are the means for the Government to get started immediately. Gi ven that each agency has unique mission needs, security requirements, and IT landscape, the cloud first policy tasks each agency to think through the Strategy and evaluate its tech nology sourcing strategy so that cloud computing options are fully considered.

To guide and expedite each agency's strategy and tactics, the Government is assembling a set of programs and tools as resources to agencies. We describe these programs and tools in the remainder of this paper.

PROGRAMS AND TOOLS

Leading private sector companies have taken great strides to improve their opera ting efficiencies. Cloud technologies and Infrastructure-as-a-Service enable IT servi ces to efficiently share demand across infrastructure assets, reducing the overall reserve capacity across the enterprise. Additionally, leveraging shared services of "commodi ty" applications such as e-mail across functional organizations allows organizations to redirect management attention and resources towards value-added activities. The massive scale of the Federal Government allows for great potential to leverage these efficiencies.

The policies and plans described above outline the actionable, achievable steps to improve the Government's operational efficiency. This section describes the programs and tools that will help agencies implement three-part strategy on cloud technolo gy: using commercial cloud technologies where feasible, launching private Government clouds, and utilizing regional clouds with state and local governments where appropriate.

Apps.Gov & lnfo.Apps.Gov

Apps.gov was originally intended to be "a one-stop source for cloud services," and is designed to lower costs and push innovation into Government agencies. The site features business applications, cloud services, productivity apps and social me dia software that are pre-approved so that agencies can be confident that the offerings are already compliant with various Federal

policies. When fully populated, Apps.gov will streamline the complex Federal procurement processes that can slow down deployment.

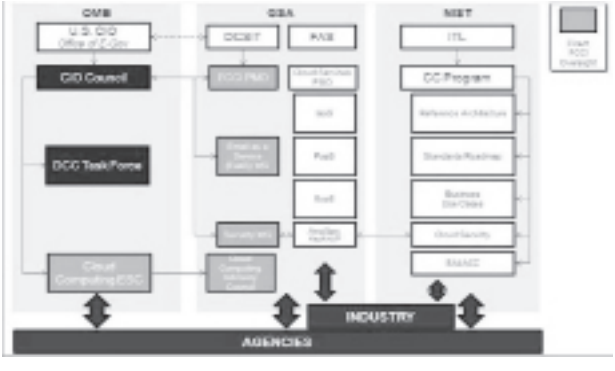
Info.Apps.gov is "a place where agencies can gather information about how cloud computing can help create sustainable, more cost-effective IT Services for the Federal Government." It is a frequently updated and authoritative source for the la test in Government news, blogs, documentation, upcoming events, and highlights on Federal cloud computing.

FCCI Governance

The mission of the Federal Cloud Computing Initiative (FCC!) is to "Drive the Government-wide adoption of cost effective, green, and sustainable Federal cloud computing solutions." The vision is to establish secure, easy to use, rapidly provisioned IT services for the Federal Government, including:

Agile and simple acquisition and certification processes
Elastic, usage-based delivery of pooled computing resources
Portable, reusable, and interoperable business-driven solutions
Browser-based ubiquitous Internet access to services
Always on and available, utility-like solutions

Figure 3. Federal Cloud Computing Initiative Governance Structure



Detailed information about FCCI governance is available at the United States General Services Administration FCCI Governance reference provided in the "Works Cited" section below. Within the governance structure, the following high-level responsibilities are assigned:

The Office of Management and Budget (OMB) coordinates activities across governance bodies, sets overall cloud-related priorities, and provides guidance to agencies.

The Federal CIO Council drives Goverment-wide adoption of cloud, identifies next-generation cloud technologies, and shares best practices and reusable example analyses and templates.
The General Service Administration (GSA) develops Goverment-wide procurement vehicles and develops Goverment-wide and cloud-based application solutions where needed
The National Institute of Standards and Technology (NIST) leads and collaborates with Federal, State, and local government agency CIOs, private sector experts, and international bodies to identify and prioritize cloud coputing standards and guidance
The Department of Homeland Security (DHS) monitors operational security issues related to the cloud
Individual Agencies are responsible for evaluating their sourcing strategies to fully consider cloud computing solutions

Collectively, the FCCI governance structure develops and delivers all of the stra tegies, planning (budget, resource, and technical), and deliverables for implementa tion of the Federal Cloud Computing Initiative, and coordinates with the Federal Enterprise Architecture for compliance, convergence, and optimization of IT Infras tructure.

FedRAMP

The Federal Information Security Management Act (FISMA) and NIST special publications provide Federal Agencies with guidance and framework needed to secu rely use cloud systems. However, interpretation and application of FISMA require ments and NIST Standards vary greatly from agency to agency. Not only do agencies have varying numbers of security requirements at or above the NIST baseline, many times additional requirements from multiple agencies are not compatible on the same system, which would make cloud computing untenable. A Government-wide risk and authorization program for cloud computing allows agencies to completely leverage the work of an already completed authorization or only require an agency to comple te delta requirements (i.e., the unique requirements for that individual agency).

The Federal Risk and Authorization Management Program (FedRAMP) has been established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. FedRAMP allows joint authorizations and continuous security monitoring services for Government and Commercial cloud com puting systems intended for multi-agency use. Joint authorization of cloud providers result in a common security risk mo-

del that can be leveraged across the Federal Go vernment. The use of this common security risk model provides a consistent base line for Cloud based technologies. This common baseline ensures that the benefits of cloud-based technologies are effectively integrated across the various cloud com puting solutions proposed within the Government. The risk model also enables the Government to "approve once, and use often" by ensuring multiple agencies gain the benefit and insight of the FedRAMP's Authorization and access to each cloud service provider's authorization package.

FedRAMP is a Government-wide initiative to provide a single set of security controls and joint authorization services up to the FISMA "Moderate" level in Fede ral Civilian agencies, and Department of Defense Information Assurance Certifica tion and Accreditation Process (DIACAP) Mission Assurance Category II Sensitive in DoD departments. It began by creating a Joint Authorization Board (JAB) defining unified, Government-wide risk management controls that work in concert with the security controls contained in NIST Special Publication 800-53, Revision 3. The JAB consists of the CIOs from DoD, DHS, GSA, and the CIO of the agency sponsoring the system to FedRAMP.

FedRAMP security requirements identify 13 additional cloud-specific control enhancements for low impact systems and approximately 60 additional control en hancements for moderate impact systems that go beyond those basic requirements defined in NIST SP 800-53.

FedRAMP is an optional service to agencies and agencies retain their responsi bility and authority to ensure that the implementation of systems meets their security needs. Assuming there are no delta requirements, the FedRAMP process consists of 9 activities:

1) The Government categorizes the information and information system.
2) The Government creates a Security Specification, including the selection of security controls.
3) The cloud provider implements the security controls.
4) An independent 3rd party assesses the security controls.
5) The cloud provider creates and authorization package.
6) The Government JAB reviews the authorization package and FedRAMP authorizes the system.
7) The Agency wishing to use the cloud provider's system provides an Agency review of the authorization package and FedRAMP Authorization, and ac cepts the authorization.
8) The cloud provider continuously monitors the security of the system and reports to FedRAMP.

9) The Government continuously monitors and accepts the ongoing level of risk.

Note that activity 5 above shifts the cost of creating the authorization package and activity 8 above shifts the cost of continuous security monitoring from the Go vernment, where it has historically been incurred, to the cloud service provider. A benefit to the cloud service provider is that they receive a common baseline of security controls that are uniformly interpreted and applied for use by multiple agencies. The cloud service provider also need only provide their sensitive security information to FedRAMP in a single format, and need not develop an individual authorization pac kage for each agency wishing to use their cloud service.

A benefit to the Agency is that a significant portion of their A&A package is provided to them by the cloud service provider when they engage the service, reducing the time and cost necessary to authorize and accredit a system using cloud services that have been FedRAMP authorized.

Additional benefits of FedRAMP include:

Increased security through focused risk management

Reduced duplication of effort

Ensured security oversight of outsourced systems

Independent accountability for Government-developed systems used by multiple agencies

Integration with Government-wide security efforts

NIST Working Groups

Cloud computing is a convergence of multiple technologies, and the descriptions, best practices, and technical standards needed to ensure cloud services are secure, per mit the Government to intemperate between multiple cloud providers (mteroperabili ty), and move data seamlessly between cloud providers (data portability) are nascent.

NIST has been designated to accelerate the Federal Government's secure adop tion of cloud computing by leading efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.

The NIST area of focus is technology, and specifically, interoperability, portability and security requirements, standards and guidance.

The intent is use the strategy to prioritize NIST tactical projects which support U.S. Government Agencies in the secure and effective adoption of the cloud compu ting model to support their missions. The expectation is that

the set of priorities ("the Roadmap") will be useful more broadly by industry, Standards Development Organi zations, cloud adopters, and policy makers.

As part of the NIST plan, five Working Groups were created as a public/private ownership to define standards.

Reference Architecture and Taxonomy WG - NIST leads interested U.S. Government agencies and industry to define a neutral cloud computing reference architecture and taxonomy to extend the NIST cloud computing model; to use as a frame of reference to facilitate communication; to illustrate and understand various cloud services in the context of an overall cloud computing model and to use as a tool to communicate and analyze candidate security, interoperability, and portability candidate standards and reference implementations.

Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC) WG - The goal of the SAJACC initiative is to drive the formation of high quality cloud computing standards by providing worked examples showing how key use cases can be supported on cloud systems that implement a set of documented and public cloud system specifications. The SAJACC initiative develops and maintains a set of cloud system use cases through an open and ongoing process engaging industry, other Government agencies, and academia.Simultaneously, the SAJACC initiative collects and generates cloud system specifications through a similarly open and ongoing process. The SAJACC initiative develops tests that show the extent to which specific use cases can be supported by cloud systems that implement documented and public cloud system specifications, and publishes test results on the SAJACC Web portal. The SAJACC web portal provides pointers to known cloud system implementations and use case documents. These resources serve to both accelerate the development of high-quality cloud computing standards and reduce technical uncertainty during the interim adoption period before many cloud computing standards are formalized.

Cloud Security WG - The formation of NIST Cloud Computing Security Working Group is an integral part of the overall NIST effort to facilitate secure adop tion of cloud services for the U.S. Government. The objectives of the WG are to gather input from all stakeholders (both within U.S. Government and Industry) regar ding security concerns in Cloud Computing Services, and to define and formulate a roadmap for development of security guidance (based on standards and best practi ces) for ensuring implementation of appropriate security controls (and their monito ring) in the cloud computing services adopted by U.S. Government agencies.

Standards Roadmap WG - NIST is leading the development of a U.S. Government Cloud Computing Roadmap. This roadmap defines and prioritizes U.S. Government requirements for interoperability, portability, and

security for cloud computing in order to support secure and industry, other Government agencies, and academia. Simultaneously, the SAJACC initiative collects and generates cloud system specifications through a similarly open and ongoing process. The SAJACC initiative develops tests that show the extent to which specific use cases can be supported by cloud systems that implement documented and public cloud system specifications, and publishes test results on the SAJACC Web portal.The SAJACC web portal provi des pointers to known cloud system implementations and use case documents. These resources serve to both accelerate the development of high-quality cloud computing standards and reduce technical uncertainty during the interim adoption period before many cloud computing standards are formalized.

Cloud Security WG - The formation of NIST Cloud Computing Security Working Group is an integral part of the overall NIST effort to facilitate secure adop tion of cloud services for the U.S. Government. The objectives of the WG are to gather input from all stakeholders (both within U.S. Government and Industry) regar ding security concerns in Cloud Computing Services, and to define and formulate a roadmap for development of security guidance (based on standards and best practi ces) for ensuring implementation of appropriate security controls (and their monito ring) in the cloud computing services adopted by U.S. Government agencies.

Standards Roadmap WG - NIST is leading the development of a U.S. Government Cloud Computing Roadmap. This roadmap defines and prioritizes U.S. Government requirements for interoperability, portability, and security for cloud com puting in order to support secure and effective U.S. Government adoption of Cloud Computing. The NIST Cloud Computing Standards Roadmap Working Group le verages existing, publicly available work, plus the work of the other NIST Working Groups, to develop a NIST Cloud Computing Standards Roadmap that can be incor porated into the U.S. Government Cloud Computing Roadmap.

Business Use Cases WG- NIST leads interested U.S. Government agencies and industry to define target U.S. Government Cloud Computing business use cases (a set of candidate deployments to be used as examples) for Cloud Computing model options, to identify specific risks, concerns and constraints. The Business Use Cases WG will: create a template for business use cases; develop target business use cases and stories; develop an in-depth use case for email; identify cross-cutting business use cases; and, coordinate with other NIST Cloud Computing working groups.

Contract Vehicles

Federal, state, and local governments will soon have access to cloud-based Infrastructure-as-a-Service (IaaS) offerings. GSA´s IaaS Blanket Purchase Agreement contract award allows 12 vendors to provide Government entities with cloud storage, virtual machines, and Web hosting services to support a continued expansion of Go vernments' IT capabilities into cloud computing environments.

After completing security certification, GSA will make a common set of contract vehicles for cloud-based Infrastructure-as-a-Service solutions available Government wide.

The Software-as-a-Service (SaaS) E-mail Working Group, formed in-June 2010, has begun to identify and develop the set of baseline functional and technical require ments for Government-wide cloud email solutions and is working towards developing business case templates for agencies who are considering transitioning to SaaS e-mail. Within 12 months, GSA will utilize these requirements to stand up Government-wide contract vehicles for cloud-based email solutions. GSA will also begin a similar pro cess specifically designed for other back-end, cloud-based solutions.

Programs And Toou; Summary

To guide and expedite each agency's strategy and tactics, the Government is assembling a set of programs and tools that are resources available to agencies to:

Expedite the process of evaluating cloud candidates, acquire cloud capability; and mitigate risk
Ensure a secure, trustworthy environment Streamline procurement processes
Establish cloud computing standards

These programs and tools serve to both accelerate the implementation of high quality cloud computing adoption and reduce technical uncertainty during the interim period before many cloud computing standards are formalized.

SUMMARY

The Federal Government's current information technology environment is cha racterized by low asset utilization, a fragmented demand for

resources, duplicative systems, environments which are difficult to manage, and long procurement lead ti mes. These inefficiencies negatively impact the Federal Government's ability to serve the American public.

Cloud computing has the potential to play a major part in addressing these in efficiencies and improving government service delivery. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly, despite resource constraints.

Commercial service providers are expanding their available cloud offerings to include the entire traditional IT stack of hardware and software infrastructure, midd leware platforms, application system components, software services, and turnkey applications. The private sector has taken advantage of these technologies to improve resource utilization, increase service responsiveness, and accrue meaningful benefits in efficiency, agility, and innovation. Similarly, for the Federal Government, cloud computing holds tremendous potential to deliver public value by increasing operatio nal efficiency and responding faster to constituent needs.

When evaluating options for new IT deployments, OMB's "cloud first" policy requires that agencies default to cloud-based solutions whenever a secure, reliable, costeffective cloud option exists. The attendant policies and plans include OMB budget guidance, the Federal Data Center Consolidation Initiative, the 25 *Point Implementation Plan to Reform Federal Irformation Technology Managemmt, and the Federal Cloud Computing Strategy.*

To facilitate the shift to cloud computing, the Government is providing agencies programs and tools, including Apps.gov, the Federal Cloud Computing Initiative governance structure, the Federal Risk and Authorization Management Program, NIST Working Groups to accelerate cloud security, interoperability, and data portability, and Federal, state, and local government contract vehicles.

The resulting Federal adoptions of cloud computing will bring a wide range of benefits, including:

Economy: Cloud computing is a pay-as-you-go approach to IT, in which a low initial investment is required to begin, and additional investment is needed only as system use increases

Flexibility: IT departments that anticipate fluctuations in user demand no longer need to scramble for additional hardware and software. With cloud computing, they can add or subtract capacity quickly and easily

Speed:Cloud computing eliminates long procurement and certification processes, while providing a near-limitless selection of services

WORK SITED

Garbars, Kurt, and Lewin, Katie, and Mell, Peter, and Tseronis, Peter. (2010) *Federal Risk and .Authorization Mano.gement Program* [online]. Available: http://csrc. nist.govIgroups/SNS/cloud-computing/documents/forumworkshop-may2010/ nist_cloud_computing_forum-mell.pdf [accessed 26 March 2011].

Kundra, Vivek. (2010) 25 *Point Implementation Plan to R4orm Federal Iriformation Tech nology Management* [online]. Available: http:/ /www.cio.gov/documents/25-Point Implementation-Plan-to-Reform-Federal%20IT.pdf [accessed 26 March 2011].

Kundra, Vivek. (2011) *Federal Cloud Crnnputing Strategy* [online]. Available: http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf [accessed 26 March 2011].

Kundra, Vivek. (26 February 2010) *Memorandumfor Chief lriformation Officers* [onli ne]. Available: http:/Iwww.cio.govIdocuments/Federal-Data-Center-Consolida tion-Initiative-02-26-2010.pdf [accessed 26 March 2011].

Kundra, Vivek. (2010) *State of Public Sector Cloud Crnnputing* [online]. Availa ble: http:I/www.cio.govIdocuments/StateOfCloudComputingReport-FI NAI..v3_508.pdf [accessed 26 March 2011].

Nationallnstitute of Standards and Technology. (2011) *Special Publication* 800-115 (Drqft): The NIST Definition of Cloud Crnnputing (Drqft) [online]. Available: http:/ I csrc.nist.govIpublications/drafts/800-145/Draft-SP-800-145_cloud-definition. pdf [accessed 26 March 2011].

United States General Services Administration. (2011) FCCI Governance [web]. Available: http:/ /info.apps.gov/node/13 [accessed 26 March 2011].

United States Office of Management and Budget (2010) *Data Center Consolidation Initiative Agency Consolidation Plan Template* [online]. Available: http:/ I cio.govIdocu ments/Data-Center-Consolidation-Plan.doc [accessed 26 March 2011].

ACRONYM LIST

A&A- Assessment and Authorization
CC- Cloud Computing
CIO - Chief Information Officer CTO - Chief Technology Officer
DCC -Data Center Consolidation
DIACAP- DoD 1A Certification and Accreditation Process

DoD- Department of Defense
DoL- Department of Labor
DHS -Department of Homeland Security
ESC -Executive Steering Committee
FAS- (GSA) Federal Acquisition Service
FedRAMP- Federal Risk and Authorization Management Program
FCCI- Federal Cloud Computing Initiative
HSMA- Federal Information Security Management Act
FY - Fiscal Year
GSA- General Services Adrnirustration
HUD- Department of Housing and Urban Development
lA - Information Assurance
IaaS - Infrastructure as a Service
IT-Information Technology
ITL- (NIST) Information Technology Laboratory
JAB -Joint Authorization Board
kWh- kilowatt hour
NIST-(U.S. Department of Conunerce) National Institute of Standards and Technology
OCSIT- (GSA) Office of Citizen Services and Innovative Technologies
OMB- (Executive Office of the President) Office of Management and Budget PaaS - Platform as a Service
PMO -Program Management Office
SaaS -Software as a Service
8.\JACC-(NIST) Standards Acceleration toJwnpstart Adoption of Cloud Computing
SLA-Service Level Agreement
TCSD - Total Cost of Service Delivery
WG- Working Group