

---

**SIIA WHITE PAPER**

---

# **Beyond the 25 Point Plan: A Roadmap to Implementing Cloud Computing and Reforming Federal IT**

---

**CLOUD COMPUTING**

---

**Software & Information  
Industry Association**  
[www.siiia.net](http://www.siiia.net)



DEVELOPED BY THE PUBLIC SECTOR INNOVATION GROUP OF THE  
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

Copyright © 2012. All rights reserved.

## Introduction

The U.S. Government is rethinking how it buys and implements IT products and services, providing agencies with the ability to purchase a broad range of IT services in a utility-based model. The Software & Information Industry Association (SIIA) produced this paper to help federal IT leaders and leading IT companies work together to comprehensively evolve the federal IT environment to catalyze government operations for the 21st Century. The ideal environment is cloud-based, agile, mobile and more cost effective.

SIIA supports the Administration's goal for federal IT leaders to focus more on mission outcomes and citizen service, by leveraging IT services as a commodity. This paper focuses on where we are today as it relates to ongoing federal IT reform, and it is useful for policymakers, government technology leaders, and the IT industry and government contractors alike. The goal of this paper is to help the Government develop an efficient IT environment and acquisition process that minimizes redundancy, delay, and administrative burden and supports agencies in the safe, secure and timely adoption of cloud computing and other innovative technologies.

In the two years since the issuance of the Federal Data Center Consolidation Initiative in February 2010 and the 25 Point Implementation Plan to Reform Federal Information Technology Management in December 2010, we have seen a dramatic movement toward the implementation of policies that reduce the cost of IT while improving service to citizens, including those aimed at promoting cloud computing. The 25 Point Plan was followed by the Cloud First Policy in July 2011, the Shared First Policy in December 2011 (as modified by the Federal IT Shared Services Strategy in May 2012) and finally the FedRAMP Concept of Operations in February 2012. Together these initiatives form the foundation of the federal government's plans to reduce its overall IT footprint and improve citizen services, while leveraging innovative technologies to reduce cost.

Taken at face value, there may appear to be some conflict between policies that ask federal agencies to both consider a move to cloud first, and also to share first, while also looking at cost effective ways to consolidate data centers. However, when you dig a little deeper, it is clear that these policies work together as "tools in a toolbox" to help federal agencies reduce cost and improve service to citizens, leveraging new and innovative technologies available as a result of the ongoing IT evolution and shift towards cloud computing.

While the decisions to use cloud computing are made at the agency level by agency Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs), the potential benefits of cloud computing cannot be fully realized if every agency independently reviews and certifies solutions. The current fragmented certification process – where agencies independently conduct certifications and accreditations on the same products – is redundant, and adds both time and cost to an already complex procurement process. This current process works counter to the nature of cloud computing and shared services.

This paper explores the inter-relationship between these existing policies, and reviews how new programs such as the Federal Risk and Authorization Management Program (FedRAMP) aim to take the issue of baseline security certification off the table, speeding

the adoption of cloud technologies in government and reducing one of the main barriers to government market entry for many contractors.

As we near the 18 month deliverables timeline on June 9, 2012, it is important to recognize that we are now at the starting line for the transformation of federal IT, not the finish line. Even as it relates to the 25 Point Plan and the “completion” of the 18 month deliverables, we have a long way to go. Many of the 25 points simply begin to put the building blocks in place, but do little to affect change. For example, the 25 Point Plan calls for a shift to a Cloud First policy. We have shifted in theory, but not one company has been certified to provide cloud computing broadly under the FedRAMP program. The Plan also calls for procurement reforms and hiring a cadre of specialized IT acquisition personnel. The plan is in place and training programs have been developed, but how many specialized IT acquisition personnel have actually been deployed? Similarly, the Plan calls for lowering the barrier of entry for small business. A lot of work has been focused on this recommendation, but has the barrier yet been lowered?

These are but a few examples of how the milestones in the original 25 Point Plan set the table for a monumental change in the federal IT landscape. Going forward, as is almost always the case, the ultimate success of the initiative will be judged not by the success of the planning but by the success of the implementation.

## Executive Summary

Beginning in early 2010 with the issuance of the Federal Data Center Consolidation Initiative, the US Government has been on a path to provide a better return on investment of its information technology spend, lower the cost of government and improve overall service to its citizens; recognizing that in the private sector cloud computing was driving innovation. The issuance of the 25 Point Implementation Plan to Reform Federal IT Management and the Cloud First Policy put IT reform front and center in the minds of decision-makers. Fast forward to today and we see a federal government that has made great strides in putting policies in place that foster the growth of cloud computing, leveraging technology to make government more efficient and effective. As we reach the 18-month deliverables deadline from the original 25 Point Plan, we see progress toward implementing cloud computing in the federal government, but significant work must be done to realize the overall vision of the 25 Point Plan.

## Transformative Benefits of Cloud Computing

As highlighted in the Federal Cloud First Strategy, “the Federal Government’s current IT environment is characterized by low asset utilization, a fragmented demand for resource, duplicative systems, environments which are difficult to manage, and long procurement lead times.” SIIA agrees that cloud computing is a key component in addressing these inefficiencies, helping agencies grappling with the need to provide highly reliable, innovative services quickly and improving government service delivery.

The transformative benefits of cloud technology, combined with its increased adoption by organizations of all sizes around the world – both private sector and government – and the demonstrated need for the federal government to reduce cost and deliver more effective services to its citizens, makes the move to speed the adoption of cloud computing in the US Government a logical and progressive step. This paper articulates how cloud computing can continue to enhance choice and lead to lower costs for the government, while also providing for better security.

## Capital Planning and Procurement

The move to cloud computing requires a monumental shift in the procurement landscape. To effectively implement the Cloud First strategy and maximize the overall return on investment of cloud computing the government needs to “buy, view and think about IT differently”, as is highlighted in the joint publication of the Chief Information Officers (CIO) and Chief Acquisition Officers (CAO) Councils, *Creating Effective Cloud Computing Contracts for the Federal Government*. This change affects four significant areas:

- **Culture:** The move to cloud computing requires a cultural shift as duties are reassigned, IT that was once provided on-site is now provided off-site and resources that have traditionally been owned by agencies are now simply utilized.

- **Developing the IT Acquisition Workforce:** The changing dynamic of the IT acquisition marketplace requires the training and deployment of specialized IT acquisition personnel, who are knowledgeable about federal acquisition rules and the changing IT marketplace.
- **Modular IT Development:** Gone are the days of buying and implementing large complex ERPs. Today's IT marketplace is driven by flexible, scalable IT projects that are developed in a modular fashion.
- **Capital Planning:** Cloud computing drives agencies away from purchasing IT in a way that requires capital expenditures and overhead, and toward an "on demand" IT model that purchases IT services as it consumes them. Capital planning guidance must keep pace with this changing dynamic.

## The Barrier of Market Entry Must Be Lowered for Small Businesses

Small businesses drive a tremendous amount of innovation throughout the IT industry. The more opportunities made available to small businesses, the more we will see innovation and sustained economic growth. In the federal government market, this means creating opportunities for success and lowering the barrier of entry for small businesses, as is called for in the 25 Point Plan. Today, while many small businesses prosper in the federal government market, most do so as subcontractors, sharing work on larger projects with traditional large government contractors. These smaller companies often shy away from pursuing work as a prime contractor because of the challenges to contracting – real or perceived – and because of the long and complex sales cycle. Lowering the barrier of entry and bringing more small businesses into the federal market would give the government increased access to innovative technology.

## FedRAMP May Create Challenges for Small Businesses

The "do once, use many times" nature of the FedRAMP process is being trumpeted by GSA as a way to reduce the cost of entry for small cloud services providers seeking to do business with the federal government. It aims to provide a portable security certification that can be used agency-to-agency, thereby eliminating the need to expend resources to meet an individual agency's security requirements. While partially true, many factors outlined in this paper show that the cost of entry for a small business under FedRAMP remains high.

## A Comprehensive IT Strategy Roadmap is Needed

The 25 Point Implementation Plan to Reform Federal IT Management, as issued in December 2010, presented a broad vision for a government that would more effectively leverage technology to reduce cost and improve service. The plan itself was too broad to affect operational change, and required the development and issuance of numerous policy memoranda to implement its vision. Over the past 18 months we have seen the issuance of the Cloud First Strategy, the Shared First/Shared Services Strategy, the Federal Data Center Consolidation Initiative and most recently the Digital Government Strategy, each with its own set of goals, requirements and milestones. Together these "strategies" form the foundation

of the federal government's plans to reduce its overall IT footprint—yet there is an inherent conflict among them.

SIIA believes that the development of a comprehensive IT strategy roadmap, along with consistent implementing guidance, will allow agencies to appropriately prioritize the multitude of ongoing IT initiatives into an operational plan that will make the original vision of the 25 Point Plan a reality.

## SIIA Recommendations At-A-Glance

### Promote a Cloud First Policy

**SIIA Recommendation #1:** The Administration should continue to promote the “Cloud First” policy as an integral part of the overall strategy to reduce the cost of government, improve the return on investment of our IT spend and improve citizen services.

### Culture and Acquisition Models Must Keep Pace with Technology

**SIIA Recommendation #2:** OMB and GSA should work together and with industry to review and recommend changes to capital planning and procurement regulations that might hinder the rapid acquisition of innovative technologies by government.

- Review the current OMB Exhibit 300 process to ensure its relevancy in today’s world of on-demand computing.

**SIIA Recommendation #3:** Promote changes to the federal acquisition process and culture that will keep pace with evolving technology. Key to this are issues raised in the original 25 Point Implementation Plan that have not yet been fully addressed:

- Develop and deploy a cadre of specialized IT acquisition professionals.
- Identify and share IT acquisition best practices.
- Develop and issue contracting guidance and templates that support modular IT development.

### Lower the Barrier of Market Entry for Small Businesses

**SIIA Recommendation #4:** Lower the barrier of entry for small innovative IT companies and make the FedRAMP process open, fair and accessible to all CSPs by fully implementing Point 16 of the 25 Point Plan.

### Develop a Comprehensive Federal IT Strategy Roadmap

**SIIA Recommendation #5:** OMB should review, revise and consolidate the policy memorandums and implementing guidance associated with the Cloud First, Shared First/ Shared Services Strategy, and the FDCCI, into a single Federal IT Strategy Roadmap.

## **Key Policy Implications & Recommendations for Implementing Federal Cloud Computing**

Over the last two years, the Administration has made great strides in fostering the growth of cloud computing to seize the economic benefits of this transformative technology, leveraging this move to create a government that is more cost effective and delivers better services to its citizens. With the approval of the first set of FedRAMP Third Party Assessors (3PAO) on May 14th, and the official launch of the FedRAMP Initial Operational Capabilities (IOC) expected the first week of June 2012, we are now at the starting line for the implementation of cloud capabilities in the federal government, a move that will turn the vision of cloud into a reality.

The work that has been performed so far provides a baseline. Going forward, SIIA believes there must be more clarity around the inter-relationship between the Cloud First, Shared First/ Shared Services strategies and the Data Center Consolidation Initiative as highlighted in this whitepaper.

The following section outlines why cloud computing is important for the federal government, identifies the key challenges hindering its implementation, and provides recommendations for how to make the cultural and strategic changes necessary for it to be adopted effectively. SIIA makes the following recommendations to help advance innovative, cloud-based federal IT Reform.

### **What is Cloud Computing and Why is it Right for the Federal Government?**

Cloud computing is not a new or singular technology, but rather an evolving mechanism for IT consumption and delivery, provisioning a wide variety of computing services from remote locations. The technology has been part of the computing landscape for decades, but with the widespread deployment of broadband communications facilities, it is increasingly within the reach of government, businesses and individual customers. At this stage in the federal government's IT development cycle, it is no longer a question of "if" the government will effectively implement cloud computing but how quickly and to what degree? Cloud computing is fast becoming mainstream in government.

While there are common definitions, the various different technologies, platforms and service models that comprise cloud computing reveal its complexity. Regardless of the challenges to define what is, or is not, "cloud computing," or the myriad platforms and service models that comprise it, cloud computing provides substantial benefits that are driving rapid adoption, including: on demand access, resource pooling, flexibility and elasticity, rapid implementation and energy efficiency, among others.

Increased adoption by organizations of all sizes around the world—both private sector and governments—has clearly demonstrated that cloud computing offers transformative benefits. For purposes of federal implementation of cloud computing, there is no question that the following two benefits are key drivers driving the transition for the federal government:



## 1. More Choice, Lower Cost:

As reliance on open standards and software and data interoperability are maximized, cloud computing can lead to greater choice and lower prices for consumers.

The movement towards cloud computing has increased the need for open standards for software and data interoperability. Open standards are critical for the successful adoption and delivery of cloud computing, which requires an environment where services can be provisioned efficiently and effectively across multiple browsers, and can run on multiple platforms such as desktop personal computers, and myriad mobile devices. There is a great promise for dramatically increasing competition among providers of computing technologies and ending the era of vendor lock-in. Over time, this will lead directly to greater choice and lower prices for consumers.

To achieve this vision, the cloud computing industry needs the flexibility to experiment to reach the most efficient and innovation-promoting degree of open standards IT architecture. To that end, the current collaborative government-industry cooperation across various forums to accelerate the standards and reference architecture development process is very promising for the mutual goal of advancing the rapid adoption and long-term effectiveness of cloud computing.

SIIA supports the central role of NIST as outlined in the Federal Cloud Computing Strategy, to define and advance standards, and to collaborate with USG agency CIOs, private sector experts, and international bodies to identify and reach consensus on cloud computing technology and standardization priorities. Indeed, NIST's leadership in identifying a set of key guidelines and recommendations for federal departments and agencies is critical to the efficient implementation of the Federal Cloud Computing Strategy.

## 2. Better Security:

Cloud computing provides an environment inherently superior for applying many critical security measures.

As complex networked systems, "clouds" are affected by traditional computer and network security issues such as the need to provide data confidentiality and maintain data integrity and system availability. While the cultural change of relinquishing direct control of the IT infrastructure has created fear for some IT professionals, there is a much less recognized reality that cloud computing, by nature, provides an environment inherently superior for applying many critical security measures. By enabling uniform security management practices, clouds are capable of improving on certain key security practices, such as predicting and detecting new threats, providing for quicker remediation, and providing for greater protection against end user breach or corruption, and lost or stolen data.

As highlighted in the Federal Cloud First Strategy (p. 1), "the Federal Government's current IT environment is characterized by low asset utilization, a fragmented demand for resource, duplicative systems, environments which are difficult to manage, and

long procurement lead times.” SIIA agrees that cloud computing is a key component in addressing these inefficiencies, helping agencies grappling with the need to provide highly reliable, innovative services quickly and improving government service delivery.

### **SIIA Recommendation #1**

The Administration should continue to promote the “Cloud First” policy as an integral part of the overall strategy to reduce the cost of government, improve the return on investment of our IT spend and improve citizen services.

As identified in the Cloud First policy, an estimated \$20 billion of the federal government’s \$80 billion IT spending is a potential target for migration to cloud computing solutions. Moving forward from the first 18-month cycle of implementation of this policy, the government should develop concrete benchmarks to meet the initial \$20 billion shift to cloud, and establish metrics for the next phase migrations.

## **Culture and Acquisition Models Must Keep Pace with Technology**

The joint publication of the Chief Information Officers (CIO) and Chief Acquisition Officers (CAO) Councils, *Creating Effective Cloud Computing Contracts for the Federal Government*, acknowledges that in order to effectively implement the “Cloud First” strategy, the “Federal Government needs to buy, view and think about IT differently.”

It’s no secret that the complexity and deliberative nature of the federal procurement processes make it difficult, costly and time consuming to pursue business with the government, driving many small and mid-sized businesses away from the federal market. It’s also no secret that the current IT acquisition processes are geared toward a different time, one in which agencies sought to acquire IT systems, servers, and other durable IT. In today’s world of cloud computing agencies are now focused on acquiring IT on demand and purchasing services and capabilities, rather than physical IT.

This change requires not only a shift in the mindset of agency leaders from thinking in terms of what capability they can have “access to,” rather than what they “own,” but also a shift in the thinking of procurement personnel to a mindset of how to leverage the existing regulations to acquire IT services quickly and cost effectively.

### **Culture is a Challenge to Federal IT Reform**

Cultural change in any organization is always a key management challenge. Issues of culture get magnified, when making a shift as dramatic as the move to cloud computing. Traditionally, most federal organizations struggle with acceptance of cultural change. With the move to cloud other issues arise as well, including: realignment of duties and organizational structure, changes to the acquisition process, and ceding control and/or ownership of resources.

Managing cultural change requires strong leadership, communication and training. Successful organizations must anticipate management challenges such as cultural resistance to change, and develop plans to mitigate these challenges.

### **Developing the IT Acquisition Workforce**

Effective IT acquisition requires not only a thorough understanding of federal acquisition practices, but also a thorough understanding of technology and the dynamic nature of the IT acquisition marketplace. As technology evolves, the federal government needs to continuously update its acquisition practices to keep pace with changing technology. The move to cloud computing represents a dramatic shift in computing and as such requires a major shift in acquisition practices to keep pace. Training or re-training IT acquisition professionals and developing a specialized cadre of IT acquisition professionals is key to the successful implementation of cloud computing in the federal government.

### **Establish Best Practices for Modular IT Development**

Acquiring cloud computing technology is inherently different than acquiring traditional IT hardware and services. Traditionally, IT acquisition has been focused on the purchase of large complex ERPs and similar systems designed to maximum capacity, regardless of whether or not to agency would utilize 100 percent of the system's capacity. Today, with the advent of cloud computing, the federal government can design, acquire and implement IT solutions in a modular fashion, providing a flexible, scalable IT environment. Modular development also dramatically changes the timeline for IT acquisition and deployment – reducing what once took years, to months, weeks, days or even hours.

The government must evolve the way it procures IT to maximize capacity, flexibility and return on investment. The federal government does not have much history with contracting for modularly developed IT solutions and therefore, changes, guidance and the identification of best practices for modular IT acquisition are needed to support this process.

### **Evolve Capital Planning to Take Advantage of Today's IT Opportunities**

The OMB Exhibit 300 process was designed for a now somewhat obsolete era of IT acquisition. Agencies must now move away from “purchasing IT in a way that requires capital expenditures and overhead and instead purchasing IT ‘on demand’ as an agency consumes services,” as is outlined in the joint report of the CIO and CAO Councils. SIIA believes that for this transformation to work in practice, the federal government must adjust not only its acquisition culture, but the agency capital planning process, as required by OMB Circular A-11 Part 7 Planning, Budgeting, Acquisition, and Management of Capital Assets. Furthermore, we believe that OMB should clarify that acquiring IT as a Service, whether defined as Software as a Service, Infrastructure as a Service, or Platform as a Service, in most cases should not require a capital budget. SIIA encourages a review of the Exhibit 300 process to ensure it is properly aligned with the overall goals of the Federal Cloud Computing Strategy.

**SIIA Recommendation #2**

OMB and GSA should work together and with industry to review and recommend changes to capital planning and procurement regulations that might hinder the rapid acquisition of innovative technologies by government.

- Review Circular A-11, Part 7, Section 300 – Planning, Budgeting, Acquisition and Management of Capital Assets (the OMB Exhibit 300 process) to ensure its relevancy in today's world of on-demand computing and highlighting best practices.

**SIIA Recommendation #3**

Promote changes to the federal acquisition process and culture that will keep pace with evolving technology. Key to this are issues raised in the original 25 Point Implementation Plan that have not yet been fully addressed:

- Support efforts to design and develop a cadre of specialized IT professionals, trained to understand the administration and management of IT as a Service contracts. More important than the simple design of this program, however, is the rapid deployment of these professionals into the IT workforce, so that the practices taught can be incorporated into the acquisition process.
- Implement government-wide effort to identify and share IT acquisition best practices.
- Develop and issue contracting guidance and templates that support modular IT development.

**Lowering the Barrier of Market Entry for Small Businesses**

Small businesses drive a tremendous amount of innovation throughout the IT industry. The more opportunities that can be available for small businesses, the more we will see sustained economic growth. In the federal government market, this means creating opportunities for success and lowering the barrier of entry for small businesses, as is called for in the 25 Point Plan.

Today, while many small businesses prosper in the federal government market, most do so as subcontractors, sharing work on larger projects with traditional large government contractors. These smaller companies often shy away from pursuing work as a prime contractor because of the barriers to contracting and because of the long and complex sales cycle. Also, affecting a small business's decision to engage in the federal procurement process is the sheer size of federal procurements, often much larger than any one small business can handle. As a result, many small businesses choose not to try to do business with the federal government, and

instead focus their efforts on the private sector. As a result, the government misses out on the advantages provided by these innovative new technologies. Modular IT development, *i.e.* breaking projects down into sizable bites, would go a long way to opening the federal market to small businesses.

### **Promoting Small Business Participation in FedRAMP**

GSA points out in its FAQs for FedRAMP that the “do once, use many times” aspect of the FedRAMP process may actually help smaller CSPs seeking to do business with the federal government by eliminating the need to expend resources for security authorizations with each federal customer. While part of this is true, in some ways FedRAMP creates additional challenges for all CSPs seeking certification under FedRAMP, with a greater burden on small businesses. More must be done to address these concerns.

Under the current FISMA requirements, any company desiring to provide IT services to the federal government must meet FISMA standards, working directly with their customer agency to receive their formal Authority to Operate (ATO). Under the proposed FedRAMP certification process, that same company can work with a 3PAO to receive a provisional FedRAMP certification giving them a formal hunting license to pursue cloud opportunities in the federal government. However, the company must then work with their customer agency to receive their formal ATO, an additional and potentially costly step depending on whether or not the contracting agency accepts the FedRAMP certification. A host of recent surveys have shown that in some cases as many as 40-50% of agencies believe they have unique security requirements not met by the FedRAMP process and expect to do additional security assessments. In practice, it is likely that the FedRAMP certification process will be seen as an additional step to the certification process.

Furthermore, recent reports from GSA indicate that the FedRAMP certification process will prioritize companies already providing cloud technology services to federal agencies under the existing Infrastructure as a Service (IaaS) Blanket Purchase Agreement (BPA) awarded on October 19, 2010. It will secondarily certify vendors on GSA's upcoming Email as a Service (EaaS) contract. These companies will have a distinct market advantage over those approved later in the process, putting small businesses at a particular disadvantage.

### **SIIA Recommendation #4**

Fully implement Point 16 of the 25 Point Plan to reduce the barrier of entry for innovative IT companies.

- GSA should ensure that the FedRAMP certification process is open, fair and accessible to all cloud service providers who meet or have the potential to meet the baseline security requirements, recognizing the unique nature of what small businesses bring to the table from a cloud perspective and meeting the spirit of the 25 Point Plan by reducing the barrier to federal market entry for small IT businesses.

## Comprehensive Federal IT Strategy Roadmap and Guidance

The federal government's move to cloud computing is a logical and progressive next step, given its increased adoption by organizations of all sizes around the world both private sector and government. SIIA agrees that cloud computing for the federal government is the right step, but the 25 Point Implementation Plan to Reform federal IT Management as issued in December 2010, while innovative, is too broad to affect any operational change. As is the case with most legislative or policy changes in the federal government, it is the implementing guidance that sets the tone for operational change. While initially born from the same plan (the 25 Point Plan), the Federal Data Center Consolidation Initiative (FDCCI), Cloud First, and Shared First as modified by the Shared Services Strategy, have each spawned a life of their own and are having a significant impact on agency operations and priorities. Together these initiatives form the foundation of the federal government's plans to reduce its overall IT footprint.

Taken at face-value, there appears to be some conflict between policies that ask federal agencies to both consider a move to cloud *first* and also to share *first*, while also looking at cost effective ways to consolidate data centers. When you dig a little deeper, it is clear that these policies can and should work together as tools in a toolbox to help federal agencies reduce cost and improve service to citizens by leveraging new and innovative technologies available as a result of cloud computing.

The stand-alone nature of the guidance that implements both the Data Center Consolidation Initiative and the Shared Services Strategy does not necessarily support the overall goal of the move to cloud. It places quotas on agencies for the number of data centers to be eliminated and the number of services moved to a shared environment. This approach, while effective from a metrics standpoint, does little to improve overall IT management and governance.

Going forward, we expect to see additional innovations, including those aimed at better leveraging mobile technology and data analytics. These initiatives, like data center consolidation and shared services, are enhanced by the advent of cloud computing. As such, they should be considered as part of a broader cloud computing strategy, as opposed to independent efforts.

A broad cloud strategy, with the goal of leveraging innovative technology to reduce cost, increase the return on investment of IT spending and improve citizen services, is far more effective. Data center consolidation, shared services and whatever future IT policies are announced should be viewed as elements of this broad cloud computing strategy.

SIIA believes that the approach to reforming federal IT management as called for in the initial plan is the correct approach and encourages the OMB Office of the Federal CIO and the CIO Council to continue to promote a holistic approach to federal IT reform.

**SIIA Recommendation #5**

OMB should review, revise and consolidate the policy memorandums and implementing guidance associated with the Cloud First, Shared First/Shared Services Strategy, and the FDCCI, into a single federal IT Strategy Roadmap. This would eliminate conflicting guidance and redundancy and providing clarity to agencies on prioritization of IT projects, highlighting the complementary nature of these initiatives.