United States Government Accountability Office

GAO

Report to the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs
United States Senate

July 2012

INFORMATION TECHNOLOGY REFORM

Progress Made but Future Cloud Computing Efforts Should be Better Planned

G A O
Accountability * Integrity * Reliability

GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-756, a report to the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs
United States Senate

July 2012

INFORMATION TECHNOLOGY REFORM

Progress Made but Future Cloud Computing Efforts Should be Better Planned

Why GAO Did This Study

As part of a comprehensive effort to increase the operational efficiency of federal technology assets, federal agencies are shifting how they deploy IT services. OMB issued a "Cloud First" policy in December 2010 that requires federal agencies to implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists; and to migrate three technology services to a cloud solution by June 2012. Cloud computing provides on-demand access to a shared pool of computing resources; can be provisioned on a scalable basis; and reportedly has the potential to deliver services faster, more efficiently, and at a lower cost than custom-developed systems.

GAO was asked to (1) assess the progress selected agencies have made in implementing this policy and (2) identify challenges they are facing in implementing the policy. To do so, GAO (1) selected seven agencies, analyzed agency documentation, and interviewed agency and OMB officials; and (2) identified, assessed, and categorized common challenges.

What GAO Recommends

GAO is making recommendations to seven agencies to develop key planning information, such as estimated costs and legacy IT systems' retirement plans for existing and planned services. The agencies generally agreed with GAO's recommendations. State disagreed with one recommendation, noting that legacy retirement plans were not applicable to its existing cloud services. GAO maintains that the recommendation is applicable for reasons discussed in this report.

View GAO-12-756. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov

What GAO Found

The selected federal agencies have made progress implementing the Office of Management and Budget's (OMB) "Cloud First" policy. Consistent with this policy, each of the seven agencies[1] incorporated cloud computing requirements into their policies and processes. For example, one agency had incorporated a review of its information technology (IT) investment portfolio to identify candidates for a cloud solution into its IT plan. Further, each of the seven agencies met the OMB deadlines to identify three cloud implementations by February 2011 and to implement at least one service by December 2011. However, two agencies do not plan to meet OMB's deadline to implement three services by June 2012, but plan to do so by calendar year end, ranging from August to December. Each of the seven agencies has also identified opportunities for future cloud implementations, such as moving storage and help desk services to a cloud environment. While each of the seven agencies submitted plans to OMB for implementing the cloud solutions, all but one plan were missing key required elements. For example, 7 of the 20 plans did not include estimated costs and none of the plans for services that were to migrate existing functionality to a cloud-based service included plans for retiring or repurposing the associated legacy systems. According to agency officials, this was largely because the information was not available at the time the plans were developed. Until agencies' cloud implementations are sufficiently planned and relevant systems are retired, the benefits of federal efforts to implement cloud solutions—improved operational efficiencies and reduced costs—may be delayed or not fully realized.

GAO identified seven common challenges associated with the implementation of OMB's "Cloud First" policy.

Common Challenges to Cloud Computing

1.	Meeting Federal Security Requirements
2.	Obtaining guidance
3.	Acquiring knowledge and expertise
4.	Certifying and accrediting vendors
5.	Ensuring data portability and interoperability
6.	Overcoming cultural barriers
7.	Procuring services on a consumption (on-demand) basis

Source: GAO analysis of agency data.

Recently issued federal guidance and initiatives recognize many of these challenges, such as the National Institute of Standards and Technology standards and guidance, and the General Services Administration's program to assist federal agencies certify and accredit potential cloud service providers.

[1] The selected agencies are the Departments of Agriculture, Health and Human Services, Homeland Security, State, and Treasury; the General Services Administration and the Small Business Administration.

Contents

Tables

Figures

Abbreviations

CIO	chief information officer
DHS	Department of Homeland Security
FedRAMP	Federal Risk and Authorization Management Program
GSA	General Services Administration
HHS	Department of Health and Human Services
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SBA	Small Business Administration
SP	Special Publication
State	Department of State
Treasury	Department of the Treasury
USDA	Department of Agriculture

G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 11, 2012

The Honorable Thomas R. Carper
Chairman
The Honorable Scott P. Brown
Ranking Member
Subcommittee on Federal Financial Management, Government
Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Cloud computing is an emerging form of delivering computing services via networks with the potential to provide information technology (IT) services more quickly and at a lower cost. Cloud computing provides users with on-demand access to a shared and scalable pool of computing resources with minimal management effort or service provider interaction. It reportedly has several potential benefits, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities.

In December 2010, the Office of Management and Budget (OMB), in its 25 Point IT Reform Plan, identified cloud computing as having the potential to play a major part in achieving operational efficiencies in the federal government's IT environment, such as improving asset utilization and reducing duplicative systems.[1] To help achieve these efficiencies, OMB developed a "Cloud First" policy that requires each agency chief information officer (CIO) to fully migrate three services to a cloud solution by June 2012, and implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists.

In light of the "Cloud First" implementation requirements, you asked us to (1) assess the progress selected agencies have made in implementing the federal "Cloud First" policy and (2) identify challenges selected agencies are facing as they implement the policy.

[1] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

To address our first objective, we selected seven agencies using a combination of the size of the agencies' IT budgets and their prior experience in using cloud services.[2] We analyzed documentation from the selected agencies, including plans and progress reports submitted to OMB, which described the actions agencies have taken to migrate selected services to a cloud solution. In addition, we interviewed officials responsible for implementing the cloud solutions to determine how the services were selected and migrated. We also interviewed officials from the National Institute of Standards and Technology (NIST) and OMB to understand cloud computing standards, requirements, and guidance for federal agencies.

To address our second objective, we interviewed officials from each of the selected agencies and asked them to describe challenges associated with their implementation of cloud solutions. We then assessed and categorized the challenges and totaled the number of times each challenge was cited by agency officials. In order to identify the common challenges, we generalized challenges that were mentioned by two or more agencies. We also compared the challenges to federal guidance[3] to determine the extent to which the guidance addresses agency challenges.

We conducted this performance audit from October 2011 through July 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Further details of our objectives, scope, and methodology are in appendix I.

[2] The selected agencies are the Departments of Agriculture (USDA), Health and Human Services (HHS), Homeland Security (DHS), State, and the Treasury; the General Services Administration (GSA) and the Small Business Administration (SBA).

[3] OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011) and CIO Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service* (Feb 24, 2012).

Background

IT can enrich people's lives and improve organizational performance. For example, during the last two decades, the Internet has matured from being a means for academics and scientists to communicate with each other to being a national resource where citizens can interact with their government in many ways, including receiving services and supplying and obtaining information.

While investments in IT have the potential to improve lives and organizations, some federally funded IT projects can—and have—become risky, costly, unproductive mistakes. As part of a comprehensive effort to increase the operational efficiency of federal technology assets and deliver greater value to the American taxpayer, federal agencies are shifting to the deployment of cloud services.

Overview of Cloud Computing

Cloud computing takes advantage of several broad evolutionary trends in IT, including the use of virtualization.[4] According to NIST, cloud computing is a means "for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST also states that an application should possess five essential characteristics to be considered cloud computing: on-demand self service, broad network access, resource pooling, rapid elasticity, and measured service.[5] Essentially, cloud computing applications are network-based and scalable on demand.

[4] Virtualization is a technology that allows multiple, software-based machines, with different operating systems, to run in isolation, side-by-side, on the same physical machine. Virtual machines can be stored as files, making it possible to save a virtual machine and move it from one physical server to another. Virtualization is often used as part of cloud computing.

[5] NIST further defines these characteristics as follows. On-demand self-service allows consumers to acquire computing capabilities automatically and as needed. Broad network access provides capabilities over a network, which are accessed through standard mechanisms (e.g., mobile phones, tablets, laptops, and workstations). Resource pooling means the vendor's combined computing resources serve multiple consumers. Rapid elasticity refers to the ability to vary resources commensurate with demand. Measured services means usage is incrementally valued, typically on a pay-per-use or charge-per-use basis.

According to OMB, cloud computing brings a wide range of benefits:

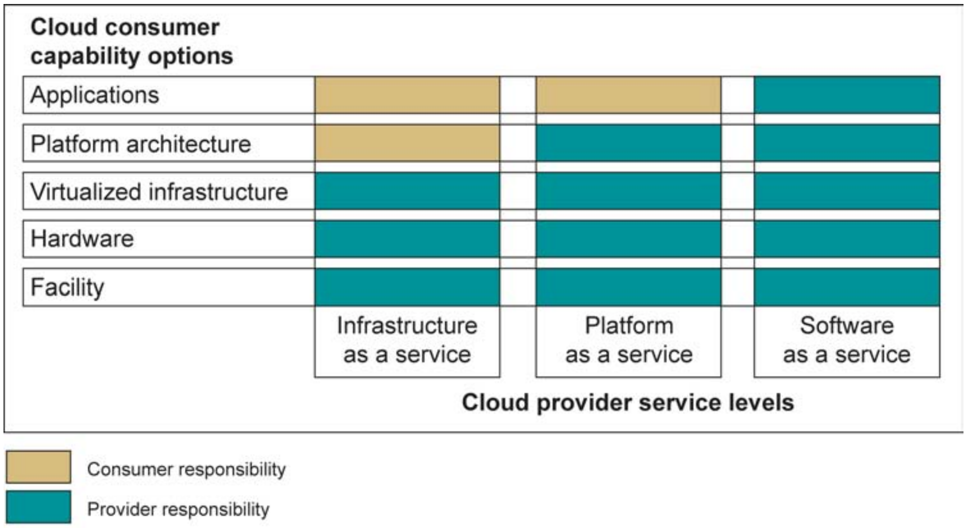
- Economical: cloud computing is a pay-as-you-go approach to IT, in which a low initial investment is required to begin, and additional investment is needed only as system use increases.
- Flexible: IT departments that anticipate fluctuations in user demand no longer need to scramble for additional hardware and software. With cloud computing, they can add or subtract capacity quickly and easily.
- Fast: cloud computing eliminates long procurement and certification processes, while providing a near-limitless selection of services.

According to NIST, cloud computing offers three service models:

- Infrastructure as a service—the service provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment upon which a platform (i.e., operating system and programming tools and services) to develop and execute applications can be developed by the consumer.
- Platform as a service—the service provider delivers and manages the underlying infrastructure (i.e., servers, software, storage, and network equipment), as well as the platform (i.e., operating system, and programming tools and services) upon which the consumer can create applications using programming tools supported by the service provider or other sources.
- Software as a service—the service provider delivers one or more applications and the computational resources and underlying infrastructure to run them for use on demand as a turnkey service.

As can be seen in figure 1 below, each service model offers unique functionality, with consumer control of the environment decreasing from infrastructure to platform to software.

Figure 1: Cloud Service Provider and Consumer Responsibilities for the Three Service Models



Cloud consumer capability options	Infrastructure as a service	Platform as a service	Software as a service
Applications	🟨	🟨	🟦
Platform architecture	🟨	🟦	🟦
Virtualized infrastructure	🟦	🟦	🟦
Hardware	🟦	🟦	🟦
Facility	🟦	🟦	🟦

Cloud provider service levels

🟨 Consumer responsibility

🟦 Provider responsibility

Source: GAO analysis based on NIST data.

NIST has also defined four deployment models for providing cloud services: private, community, public, and hybrid.

- In a private cloud, the service is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the customer’s premises.
- In a community cloud, the service is set up for organizations with similar requirements. The cloud may be managed by the organizations or a third party and may exist on or off the organization’s premises.
- A public cloud is available to the general public and is owned and operated by the service provider.
- A hybrid cloud is a composite of two or more of the above deployment models (private, community, or public) that are bound together by standardized or proprietary technology that enables data and application portability.

According to federal guidance, these deployment models determine the number of consumers (tenancy), and the nature of other consumers’ data that may be present in a cloud environment. A public cloud should not allow a consumer to know or control other consumers of a cloud service provider’s environment. However, a private cloud can allow for ultimate control in selecting who has access to a cloud environment. Community clouds and hybrid clouds allow for a mixed degree of control and knowledge of other consumers. Additionally, the cost for cloud services typically increases as control over other consumers and knowledge of these consumers increase.

Federal Guidance for Cloud Computing

According to OMB, the federal government needs to shift from building custom systems to adopting cloud technologies and shared solutions, which will improve the government's operational efficiencies and result in substantial cost savings. To achieve these benefits, OMB required agencies to immediately shift to a "Cloud First" policy and increase their use of available cloud and shared services whenever a secure, reliable, and cost-effective cloud solution exists.

In order to accelerate the adoption of cloud computing solutions across the government, OMB made cloud computing an integral part of its *25 Point Implementation Plan to Reform Federal Information Technology Management*.[6] The plan specified six major goals:

- strengthen program management,
- streamline governance and improve accountability,
- increase engagement with industry,
- align the acquisition process with the technology cycle,
- align the budget process with the technology cycle, and
- apply "light technology" and shared solutions.[7]

To achieve these goals, the plan outlines 25 action items, such as completing plans to consolidate 800 data centers by 2015[8] and developing a governmentwide strategy to hasten the adoption of cloud computing. To accelerate the shift to cloud computing, OMB required agencies to identify, plan, and fully migrate three services to a cloud solution by June 2012.

[6] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington D.C.: Dec. 9, 2010).

[7] According to OMB, "light technologies" are cloud services.

[8] As of December 2011, OMB plans to consolidate 1,200 data centers by 2015.

In February 2011, OMB issued the *Federal Cloud Computing Strategy*, as called for in its 25-Point Plan.[9] The strategy provides definitions of cloud computing; benefits of cloud computing, such as accelerating data center consolidations; a decision framework for migrating services to a cloud environment;[10] case studies to support agencies' migration to cloud computing; and roles and responsibilities for federal agencies. For example, the strategy states that NIST's role is to lead and collaborate with federal, state, and local government agency CIOs, private sector experts, and international bodies to identify and prioritize cloud computing standards and guidance. Further, the strategy notes that an estimated $20 billion of the federal government's $80 billion in annual IT spending is a potential target for migration to cloud computing solutions.

In a December 2011 memo, OMB established the Federal Risk and Authorization Management Program (FedRAMP), a governmentwide program to provide joint authorizations and continuous security monitoring services for all federal agencies.[11] Among other things, the memo required the General Services Administration's (GSA) FedRAMP program management office to publish a concept of operations, which was completed in February 2012. The concept of operations states that FedRAMP is to:[12]

- ensure that cloud-based services have adequate information security;
- eliminate the duplication of effort and reduce risk management costs; and
- enable rapid and cost-effective procurement of information systems/service for federal agencies.

[9] OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

[10] The decision framework, among other things, identifies several key areas for determining the readiness for moving to a cloud environment, including the ability of the cloud service provider to address government security requirements.

[11] OMB, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011). The FedRAMP program is governed by the Joint Authorization Board (composed of the CIOs from the Departments of Defense and Homeland Security, and GSA), the FedRAMP program management office, NIST, the Federal CIO Council, OMB, and the Department of Homeland Security.

[12] GSA, *FedRAMP Concept of Operations (CONOPS) version 1.0* (Feb. 7, 2012).

Further, the FedRAMP program is to assess and grant cloud service providers provisional authorization to provide cloud services governmentwide. Agencies can leverage the provisional authorization to minimize certification and accreditation processes.[13] FedRAMP reached initial operational capabilities in June 2012 and is to be fully operational in fiscal year 2014.

Consistent with OMB's Cloud Computing Strategy, NIST has issued several key publications related to standards and security. For example:

- NIST Special Publication (SP) 500-291, *NIST Cloud Computing Standards Roadmap* identifies current standards, standards gaps, and standardization priorities.[14] For example, it describes the status of cloud computing standards for interoperability, portability, and security.
- NIST SP 500-292, *NIST Cloud Computing Reference Architecture* presents the NIST Cloud Computing Reference Architecture and Taxonomy to communicate the components and offerings of cloud computing.[15] The architecture is presented in two parts: (1) a complete overview of roles; and (2) the necessary components for managing and providing cloud services, such as service deployment, service orchestration, cloud service management, security and privacy.
- NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* provides an overview of public cloud computing and the security and privacy considerations involved.[16] Specifically, the document describes the threats, technology risks, and safeguards surrounding public cloud environments, and their treatment.

[13] OMB information security policy requires agency management officials to formally authorize each of their information systems to process, store, or transmit information, and to accept the risk associated with their operation. This authorization (*accreditation*) decision is to be supported by a formal technical evaluation (*certification*) of the management, operational, and technical controls established in an information system's security plan.

[14] NIST*, Cloud Computing Standards Roadmap*, NIST SP 500-291 (Gaithersburg, Md.: July 2011).

[15] NIST*, Cloud Computing Reference Architecture*, NIST SP 500-292 (Gaithersburg, Md.: September 2011).

[16] NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST SP 800-144 (Gaithersburg, Md.: December 2011).

- NIST SP 800-145, *The NIST Definition of Cloud Computing* defines cloud computing in terms of essential characteristics, service models, and deployment models.[17]

NIST is also working on the *Cloud Computing Technology Roadmap* (SP 500-293), which is to describe cloud computing security challenges and high-priority gaps for which new or revised standards, guidance, and technology need to be developed.[18] According to NIST officials, NIST plans to publish the roadmap by the end of 2012.

In February 2012, the CIO Council and the Chief Acquisition Officers Council issued guidance for acquiring IT in a cloud environment.[19] The guidance identifies 10 key areas unique to federal agencies' procurement of cloud services that require improved collaboration and alignment during the contracting process. The 10 areas are:

- Selecting a cloud service—choosing the appropriate cloud service and deployment model.
- Cloud service provider and end-user agreements—terms of service, and service provider and end-user agreements need to be fully integrated into cloud contacts.
- Service-level agreements—agreements need to define performance with clear terms and definitions, demonstrate how performance is being measured, and identify what enforcement mechanisms are in place to ensure the conditions are met.
- Roles and responsibilities—cloud service provider, agency, and integrator roles and responsibilities should be clearly defined.
- Standards—NIST's cloud reference architecture should be used for cloud procurements.

[17] NIST, *The NIST Definition of Cloud Computing*, NIST SP 800-145 (Gaithersburg, Md.: September 2011).

[18] NIST, *U.S. Government Cloud Computing Technology Roadmap (Draft),* NIST SP 500-293 (Gaithersburg, Md.: November 2011).

[19] CIO council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service* (Feb. 24, 2012). The CIO Council and the federal CIO establish standards against which the success of agency programs can be measured, including monitoring performance, optimizing investments, and adopting and sharing best practices. The Chief Acquisition Officers Council is the principal interagency forum for monitoring and improving the federal acquisition system.

- Security—requirements for the service provider to maintain the security and integrity of the agency data must be clearly defined.
- Privacy—privacy risks and responsibilities need to be addressed in the contract between federal agencies and service providers.
- E-discovery—service providers need to be aware of the need to locate, preserve, collect, process, review, and produce electronically stored information in the event of civil litigation or investigation.
- Freedom of Information Act (FOIA)—all relevant data must be available for appropriate handling under the act.
- E-records—agencies need to ensure that service providers understand the federal agencies obligations under the Federal Records Act.[20]

More recently in May 2012, OMB issued its shared services strategy, as called for in its 25-Point Plan.[21] According to OMB, this strategy is to help federal agencies (1) improve return on investment across the agency's IT portfolio, (2) close productivity gaps by implementing integrated governance processes and innovative IT service solutions, and (3) increase communications with stakeholders to ensure transparency, accountability, and collaboration in the full life cycle of IT shared services. To facilitate these improvements, the strategy provides definitions, concepts, and critical success factors to be considered when implementing IT shared services; an implementation strategy; and a federal governance structure to support federal agencies' shared services development and implementation efforts.

Prior GAO Work Has Identified Improvements Needed in Federal Cloud Computing Efforts

In May 2010, we reported on the efforts of multiple agencies to ensure the security of governmentwide cloud computing.[22] We noted that while OMB, GSA, and NIST had initiated efforts to ensure secure cloud computing, significant work remained to be completed. For example, OMB had not yet finished a cloud computing strategy; GSA had begun a procurement for expanding cloud computing services, but had not yet developed

[20] Under the Federal Records Act of 1950, agencies are to manage the creation, maintenance, use, and disposition of records in order to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of agency operations.

[21] OMB, *Federal Information Technology Shared Services Strategy* (May 2, 2012).

[22] GAO, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, GAO-10-513 (Washington, D.C.: May 27, 2010).

specific plans for establishing a shared information security assessment and authorization process; and NIST had not yet issued cloud-specific security guidance. We made several recommendations to address these issues. Specifically, we recommended that OMB establish milestones to complete a strategy for federal cloud computing and ensure it addressed information security challenges. These include having a process to assess vendor compliance with government information security requirements and the division of information security responsibilities between the customer and vendor. OMB subsequently published a strategy in February 2011 that addressed the importance of information security when using cloud computing, but did not fully address several key challenges confronting agencies, such as the appropriate use of attestation standards for control assessments of cloud computing service providers, and the division of information security-related responsibilities between customer and provider. We also recommended that GSA consider security in its procurement for cloud services, including consideration of a shared assessment and authorization process. GSA has since developed its FedRAMP program, an assessment and authorization process for systems shared among federal agencies. Finally, we recommended that NIST issue guidance specific to cloud computing security. As noted previously, NIST has since issued multiple publications that address such guidance.

More recently, in October 2011, we testified that 22 of 24 major federal agencies reported that they were either concerned or very concerned about the potential information security risks associated with cloud computing.[23] These risks include being dependent on the security practices and assurances of vendors and the sharing of computing resources. We stated that these risks may vary based on the cloud deployment model. Private clouds, whereby the service is set up specifically for one organization, may have a lower threat exposure than public clouds, whereby the service is available to any paying customer. Evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation.

We also reported that the Federal CIO Council had established a cloud computing Executive Steering Committee to promote the use of cloud

[23] GAO, *Information Security: Additional Guidance Needed to Address Cloud Computing Concerns,* GAO-12-130T (Washington, D.C.: Oct. 6, 2011).

computing in the federal government, with technical and administrative support provided by GSA's cloud computing program management office, but had not finalized key processes or guidance. The subgroup had worked with its members to define interagency security requirements for cloud systems and services and related information security controls.

Additionally, in April 2012, we reported that more needed to be done to implement OMB's 25-Point Plan and measure its results.[24] Among other things, we reported that of the 10 key action items that we reviewed, 3 had been completed and 7 had been partially completed by December 2011. In particular, OMB and agencies' cloud-related efforts only partially addressed requirements. Specifically, agencies' plans were missing key elements, such as a discussion of needed resources, migration schedules, or plans for retiring legacy systems. As a result, we recommended, among other things, that the Secretaries of Homeland Security, Veterans Affairs, and the Attorney General direct their respective CIOs to complete elements missing from the agencies' plans for migrating services to a cloud computing environment. In comments on a draft of this report, each of the agencies generally agreed with our recommendations.

[24] GAO, *Information Technology Reform: Progress Made; More Needs to Be Done to Complete Actions and Measure Results*, GAO-12-461 (Washington, D.C.: Apr. 26, 2012).

Agencies Have Made Progress Implementing OMB's Cloud First Policy, but Better Planning Is Needed for Future Efforts

OMB requires federal agencies to immediately shift to a "Cloud First" policy by implementing cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists.[25] To accelerate the shift, OMB required agencies, by February 2011, to identify three IT services to be migrated to a cloud solution and develop a plan for each of the three services, migrate one of the services to a cloud-based solution by December 2011, and migrate the remaining services by June 2012.[26] According to OMB's 25-Point Plan, migrating these services was intended to build capabilities and momentum in the federal agencies, and to act as a catalyst for agencies to migrate additional services to cloud-based solutions in order to improve the government's operational efficiency and to reduce operating costs.

Each of the seven agencies we reviewed has made progress implementing OMB's "Cloud First" policy.

- Each agency has incorporated cloud computing requirements into its policies and processes. For example, the Department of State (State) incorporated into its plan a review of its IT investment portfolio to identify candidates for cloud solutions.[27] Similarly, the Department of Agriculture (USDA) identified cloud computing as a high-priority initiative and adopted the "Cloud First" policy of migrating existing, or offering new, IT services to a cloud-based environment. The agency is also developing and deploying an infrastructure to offer cloud-based services to other government departments and agencies.[28]

- Each agency identified at least three services by February 2011 to implement in a cloud environment and reported that the agency had

[25] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010) and *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

[26] While the 25-Point Plan focused on migrating existing systems to cloud-based solutions, OMB officials stated that agencies development and implementation of new services is consistent with the plan.

[27] State, *Information Technology Tactical Plan Fiscal Years 2011-2013* (Washington, D.C.: June 3, 2011).

[28] USDA, *Enterprise Architecture Transition Plan* (Washington, D.C.: June 2011). USDA's National Information Technology Center's enterprise data center is a federally owned cloud service provider that offers both infrastructure and platform cloud services.

implemented at least one cloud service by December 2011.[29] Agencies selected the services based on a mix of criteria, including (1) services that had already been implemented in a cloud environment or were in the process, (2) risk to mission functionality, and (3) maturity of the cloud solutions. In selecting the services, most agencies chose existing services, while others developed and implemented new services. Specifically, of the 21 services selected, 13 were migrations of existing functionality and 8 were new services.[30] The most commonly identified services were e-mail, website hosting, and collaboration services.

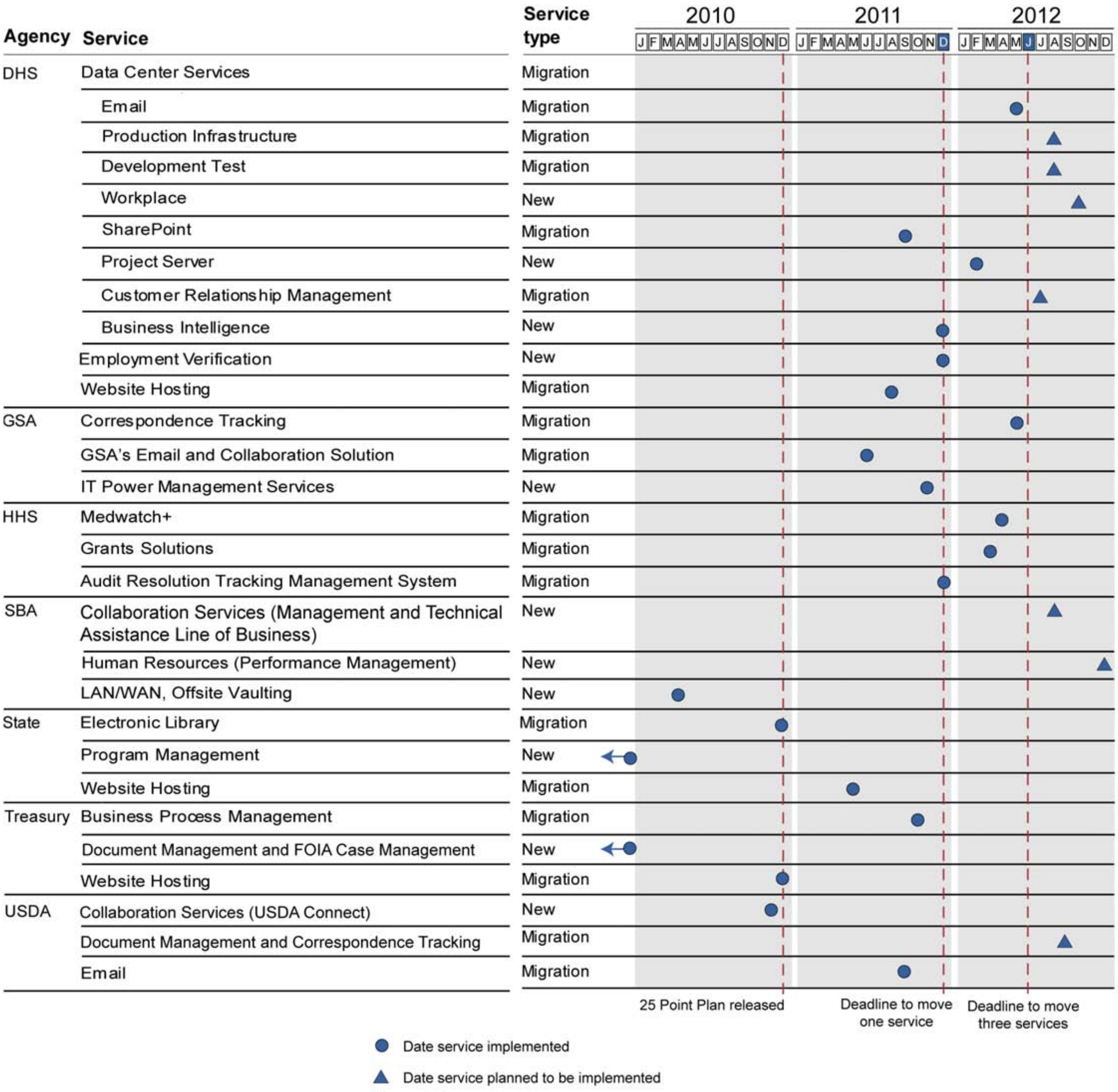
Further, five agencies reported implementing more than one cloud service by December 2011, with four agencies reporting to have implemented cloud-based services prior to December 2010, which was when OMB issued its 25-Point Plan. In addition, two of the seven agencies do not plan to meet OMB's deadline to implement three cloud solutions by June 2012. Specifically, USDA plans to complete its Document Management and Correspondence Tracking system in September 2012 and the Small Business Administration (SBA) plans to complete one of its services in August 2012 and another in December 2012.[31] While DHS does not plan to implement four of its services until after June 2012, officials reported that it implemented four services by December 2011 and two services by June 2012. See figure 2 for the cloud-based services by agency and service type; and reported planned and implementation dates.

[29] See app. II for additional details on the 21 selected services.

[30] One of DHS's selected services, Data Center Services, encompasses eight cloud services that are to improve collaboration and enhance sharing of sensitive information within the department. Additionally, Treasury initially identified Data Center Services (part of the Consumer Financial Protection Bureau) to move to a cloud solution, but officials reported that it is no longer part of Treasury's infrastructure and not under their authority. Therefore, we have not included it in our review.

[31] In May 2012, USDA's Associate CIO stated that USDA submitted another cloud initiative to meet OMB's requirement to migrate three services by June 2012. This additional service migrated disparate, localized and agency-specific tools into a centralized tool to manage FOIA requests.

Figure 2: Agencies' Cloud-based Services by Service Type and Reported Planned and Implementation Dates



Agency	Service	Service type
DHS	Data Center Services	Migration
	Email	Migration
	Production Infrastructure	Migration
	Development Test	Migration
	Workplace	New
	SharePoint	Migration
	Project Server	New
	Customer Relationship Management	Migration
	Business Intelligence	New
	Employment Verification	New
	Website Hosting	Migration
GSA	Correspondence Tracking	Migration
	GSA's Email and Collaboration Solution	Migration
	IT Power Management Services	New
HHS	Medwatch+	Migration
	Grants Solutions	Migration
	Audit Resolution Tracking Management System	Migration
SBA	Collaboration Services (Management and Technical Assistance Line of Business)	New
	Human Resources (Performance Management)	New
	LAN/WAN, Offsite Vaulting	New
State	Electronic Library	Migration
	Program Management	New
	Website Hosting	Migration
Treasury	Business Process Management	Migration
	Document Management and FOIA Case Management	New
	Website Hosting	Migration
USDA	Collaboration Services (USDA Connect)	New
	Document Management and Correspondence Tracking	Migration
	Email	Migration

● Date service implemented

▲ Date service planned to be implemented

Source: GAO analysis based on agency data.

While each agency submitted plans to OMB for its selected services, all but 1 of the 20 plans submitted to OMB were missing one or more key required elements.[32] In its 25-Point Plan, OMB required agencies to prepare a plan for implementing each cloud-based service and retiring the associated legacy system. According to OMB, each plan is to contain, among other things, estimated costs of the service, major milestones, and performance goals. However, only 1 plan fully met the key elements as required. For example, of the 20 plans, 7 did not include estimated costs, 5 did not include major milestones, and 11 did not include performance goals. Further, none of the 14 projects migrating existing services included plans to retire the associated legacy systems. See table 1 for our assessment of key elements of the agencies' plans.

[32] DHS submitted a single plan to OMB for its eight Data Center Services. SBA had initially submitted a plan to OMB for its Website Hosting service, but later changed its selection, opting instead to implement the LAN/WAN Offsite Vaulting service. SBA officials stated that they did not submit a plan to OMB for this new service. Therefore, we only reviewed plans for two of the three SBA services.

Table 1: Assessment of Key Elements of Selected Agencies’ Plans

Agency	Service	Estimated costs	Major milestones	Performance goals	Retirement Plans
DHS	Data Center Services		✓		
	Employment Verification		✓		n/a[a]
	Website Hosting	✓	✓	✓	
GSA	Correspondence Tracking	✓	✓		
	GSA's E-mail and Collaboration Solution	✓	✓		
	IT Power Management Services	✓	✓		n/a
HHS	Medwatch+	✓		✓	
	Grants Solutions	✓	✓		
	Audit Resolution Tracking Management System	✓	✓	✓	
SBA	Collaboration Services (Management and Technical Assistance Line of Business)		✓		n/a
	Human Resources (Performance Management)		✓		n/a
State	Electronic Library	✓	✓		
	Program Management	✓	✓	✓	
	Website Hosting	✓	✓	✓	
Treasury	Business Process Management	✓		✓	
	Document Management and FOIA Case Management	✓	✓	✓	n/a
	Website Hosting	✓		✓	
USDA	Collaboration Services (USDA Connect)				n/a
	Document Management and Correspondence Tracking		✓		
	E-mail			✓	

Source: GAO analysis of agency data.

[a] Services providing new functionality would not have a plan to retire associated legacy systems.

While agencies did not include all of these elements in the plans provided to OMB, three agencies later reported that they had estimated costs for five of the seven services. According to agency officials, information was missing because it was not available at the time the plans were submitted to OMB or it was deemed not to be relevant.

While developing milestones for services already implemented would appear to add little value, it remains important that agencies develop cost estimates, performance goals, and plans to retire associated legacy systems. Doing so would enable agencies to measure performance and determine whether the cloud-based solution is cost effective, and ensure that savings generated from retiring systems are realized.

Additionally, each of the agencies identified opportunities for future cloud implementations. For example, GSA officials stated that GSA is considering migrating its storage and help desk services to the cloud, while State officials stated that the agency is considering moving its development environment to a cloud solution. Further, USDA is currently offering a portfolio of cloud services to other agencies through its National Information Technology Center, which, according to USDA officials, is working to provide competitive and scalable services to federal agencies.

As agencies implement these and other cloud-based solutions, identifying key information—cost estimates, milestones, performance goals, and legacy system retirement plans—will also be essential in determining whether their activities constitute a positive return on investment, and therefore, whether the benefits of their activities will be fully realized.

Several Challenges Affected Agencies' Implementation of the Cloud First Policy

In transitioning to cloud-based solutions, officials in the agencies we reviewed stated that they encountered challenges that may impede their ability to realize the full benefits of cloud-based solutions:

- *Meeting federal security requirements*: Cloud vendors may not be familiar with security requirements that are unique to government agencies, such as continuous monitoring and maintaining an inventory of systems. For example, State officials described their ability to monitor their systems in real time, which they said cloud service providers were unable to match. Treasury officials also explained that the Federal Information Security Management Act's requirement of maintaining a physical inventory is challenging in a cloud environment because the agency does not have insight into the provider's infrastructure and assets.
- *Obtaining guidance*: Existing federal guidance for using cloud services may be insufficient or incomplete. Agencies cited a number of areas where additional guidance is needed such as purchasing commodity IT and assessing Federal Information Security Management Act

security levels.[33] For example, an HHS official noted that the 25-Point Plan required agencies to move to cloud-based solutions before guidance on how to implement it was available. As a result, some HHS operating divisions were reluctant to move to a cloud environment. In addition, Treasury officials noted confusion over NIST definitions of the cloud deployment models, but noted that recent NIST guidance has been more stable.

- *Acquiring knowledge and expertise*: Agencies may not have the necessary tools or resources, such as expertise among staff, to implement cloud solutions. DHS officials explained that delivering cloud services without direct knowledge of the technologies has been difficult. Similarly, an HHS official stated that teaching their staff an entirely new set of processes and tools—such as monitoring performance in a cloud environment—has been a challenge.
- *Certifying and accrediting vendors*: Agencies may not have a mechanism for certifying that vendors meet standards for security, in part because the Federal Risk and Authorization Management Program (FedRAMP) had not yet reached initial operational capabilities.[34] For example, GSA officials stated that the process to certify Google to meet government standards for their migration to cloud-based e-mail was a challenge. They explained that, contrary to traditional computing solutions, agencies must certify an entire cloud vendor's infrastructure. In Google's case, it took GSA more than a year to certify more than 200 Google employees and the entire organization's infrastructure (including hundreds of thousands of servers) before GSA could use Google's service.
- *Ensuring data portability and interoperability*: To preserve their ability to change vendors in the future, agencies may attempt to avoid platforms or technologies that "lock" customers into a particular product. For example, a Treasury official explained that it is challenging to separate from a vendor, in part due to a lack of visibility into the vendor's infrastructure and data.

[33] As required under the Federal Information Security Management Act of 2002, NIST guidance defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The three potential impact levels of a breach are: low (limited adverse effect), moderate (serious adverse effect), and high (catastrophic adverse effect).

[34] FedRAMP reached initial operational capabilities in June 2012. According to OMB, FedRAMP will reduce duplicative efforts, inconsistencies, and cost inefficiencies associated with the current security authorization process.

- *Overcoming cultural barriers*: Agency culture may act as an obstacle to implementing cloud solutions. For example, a State official explained that public leaks of sensitive information have put the agency on a more risk-averse footing, which makes it more reluctant to migrate to a cloud solution.
- *Procuring services on a consumption (on-demand) basis*: Because of the on-demand, scalable nature of cloud services, it can be difficult to define specific quantities and costs. These uncertainties make contracting and budgeting difficult due to the fluctuating costs associated with scalable and incremental cloud service procurements. For example, HHS officials explained that it is difficult to budget for a service that could consume several months of budget in a few days of heavy use.

Recently issued federal guidance and initiatives recognize many of these challenges. For example, OMB's *Federal Cloud Computing Strategy* recognizes the challenge of data portability and interoperability and notes that agencies should consider the availability of technical standards for cloud interfaces that reduce the risk of vendor lock-in.[35] Similarly, several NIST publications—such as their *Guidelines on Security and Privacy in Public Cloud Computing and Cloud Computing Reference Architecture*—address portability, interoperability, and security standards, and NIST plans to issue additional guidance on cloud computing security, among other things.[36] In addition, the FedRAMP program is to create processes for security authorizations and allow agencies to leverage security authorizations on a governmentwide basis in an effort to streamline the certification and accreditation processes.

Conclusions

Selected agencies have made progress implementing OMB's "Cloud First" policy. In particular, agencies have incorporated cloud solutions into their IT and investment management policies and processes, and implemented one or more services in a cloud environment by December 2011. Two agencies do not plan to meet OMB's requirement to fully implement three services to a cloud environment by June 2012, but plan to do so by year end.

[35] OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

[36] NIST, SP-800-144 (December 2011) and SP 500-292 (September 2011).

Further, agencies' plans for implementing these services were often missing key information, such as performance goals or legacy system retirement plans. Without complete information, agencies are not in a position to know whether the implementation of the selected services was cost-effective and whether the cost savings generated from retiring legacy systems were realized. Going forward, as agencies implement additional cloud-based solutions, it is important that, at a minimum, they develop estimated costs, milestones, performance goals, and plans for retiring relevant legacy systems. Until agencies' cloud implementations are sufficiently planned and relevant systems are retired, the benefits of federal efforts to implement cloud solutions—improved operational efficiencies and reduced costs associated with retiring legacy systems—may be delayed or not fully realized.

Additionally, agencies are facing a series of challenges as they implement cloud solutions. Recent guidance and initiatives may help to mitigate the impact of these challenges. Further, these initiatives may help agencies assess their readiness to implement cloud-based solutions and guide their implementation.

Recommendations for Executive Action

To help ensure the success of agencies' implementation of cloud-based solutions, we are recommending that the Secretaries of Agriculture, Health and Human Services, Homeland Security, State, and the Treasury; and the Administrators of the General Services Administration and Small Business Administration direct their respective CIOs to take the following two actions:

- establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed in this report, as applicable; and
- develop, at a minimum, estimated costs, milestones, performance goals, and plans for retiring legacy systems, as applicable, for planned additional cloud-based services.

Agency Comments and Our Evaluation

We received comments on a draft of this report from all seven departments and agencies in our review, as well as from OMB and NIST. The Departments of Agriculture, Homeland Security, and Treasury, and the GSA agreed with our recommendations; the Department of State agreed with our second recommendation and disagreed with our first recommendation; and HHS and SBA did not agree or disagree with our recommendations. Each agency's comments are discussed in more detail below.

- In written comments, USDA's Acting CIO stated that the department concurred with the content of the report and had no comments. USDA's written comments are provided in appendix III.

- In written comments, the Director of DHS's GAO-OIG Liaison Office concurred with our recommendations and described ongoing and planned actions to address them. DHS's written comments are provided in appendix IV. The department also provided technical comments, which we have incorporated in the report as appropriate.

- In comments provided via e-mail, Treasury's Deputy Assistant Secretary for Information Systems stated that the department agreed with the report and had no comments.

- In written comments, GSA's Acting Administrator agreed with our findings and recommendations, and stated that GSA will take action as appropriate. GSA's written comments are provided in appendix V.

- In written comments, State's Chief Financial Officer concurred with our recommendation to develop cost estimates, milestones, performance goals, and plans for retiring legacy systems for its planned cloud-based services. The department stated that it has established an annual requirement for all programs and initiatives to conduct an alternative analysis for retiring legacy systems and using cloud-based services, if feasible. The analysis includes the development of estimated costs, milestones, performance goals, and legacy system retirement plans. The department disagreed with our recommendation to establish cost estimates, performance goals, and plans to retire associated legacy systems for each of the department's cloud-based services discussed in this report, noting that these services did not have associated legacy systems to be retired. In a clarifying conversation, the Division Chief, Bureau of Information Resource Management, explained that one of the two migrated services ran on a virtual machine that hosts many other programs, and the other service transitioned from internally-managed software to a cloud-based service, neither of which required the retirement of an existing system. We acknowledge that a retirement plan may not be applicable for these two services; however, our recommendation is not focused solely on the need for legacy retirement plans, but also identifies the need to establish cost estimates and performance goals for each cloud-based service discussed in this report. As stated in this report, State did not establish performance goals for its electronic library service. Performance goals help to set priorities and drive progress toward key outcomes, thus enabling agencies to measure performance and determine whether the acquired cloud-based service is performing as intended and achieving the desired outcome. Therefore, we believe that the recommendation is applicable and relevant to the department. State's written comments are provided in appendix VI.

- In comments provided via e-mail, HHS's Office of the Assistant Secretary for Legislation stated that the department did not have any general or technical comments on the report.

- In comments provided via e-mail, SBA's Office of Congressional and Legislative Affairs stated that the agency had no comments on the draft report and that SBA would work to implement the recommendations.

OMB and NIST provided technical comments, which we have incorporated as appropriate.

We are sending copies of this report to interested congressional committees; the Secretaries of Agriculture, Commerce, Health and Human Services, Homeland Security, State, and the Treasury; the Administrators of the General Services Administration and Small Business Administration; the Director of the Office of Management and Budget; and other interested parties. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VII.

David A. Po

David A. Powner
Director, Information Technology
Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) assess the progress selected agencies have made in implementing the federal “Cloud First” policy and (2) identify challenges selected agencies are facing as they implement the policy.

To address our first objective, we first categorized agencies by the size of their information technology (IT) budget: large (more than $3 billion), medium ($1-3 billion), and small (less than $1 billion), as reported in the Office of Management and Budget’s (OMB) fiscal year 2011 Exhibit 53. We then selected agencies from each budget category to include (1) a mix of services (e.g., e-mail, collaboration, and website hosting) that agencies had proposed moving to the cloud and (2) agencies that were cited by OMB as having successfully implemented a cloud solution.[1] Seven agencies were selected: the Departments of Agriculture (USDA), Health and Human Services (HHS), Homeland Security (DHS), State, and the Treasury; and the General Services Administration (GSA) and the Small Business Administration (SBA). We analyzed documentation from the selected agencies, including project plans and progress reports, which described the actions agencies have taken to migrate services to a cloud solution. We also compared agencies’ migration plans to OMB’s associated guidance to determine any variances. We interviewed officials responsible for implementing the cloud solutions to determine how the services were selected and migrated. Finally, we interviewed officials from the National Institute of Standards and Technology (NIST) and OMB to understand cloud computing standards, requirements, and guidance for federal agencies.

To address our second objective, we interviewed officials from each of the selected agencies and asked them to describe challenges associated with their implementation of cloud solutions. Because of the open-ended nature of our discussions with agency officials, we conducted a content analysis of the information we received in order to identify and categorize common challenges. To do so, two team analysts independently reviewed and drafted a series of challenge statements based upon each agency’s records. They then worked together to resolve any discrepancies, choosing to report on challenges that were identified by two or more agencies. These common challenges were presented in the report. Finally, we compared the challenges to OMB’s *Federal Cloud Computing Strategy* and the Chief Information Officers Council’s and Chief

[1] The three agencies cited by OMB are USDA, HHS, and GSA.

Acquisition Officers Council's cloud computing guidance to determine the extent to which they were addressed.[2]

We conducted this performance audit from October 2011 through July 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[2] OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011) and Chief Information Officer Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service* (Feb. 24, 2012).

Appendix II: Descriptions of Selected Services

This appendix provides information on the services the selected federal agencies chose to migrate to cloud solutions. Specifically, this appendix includes a brief description of the three cloud services, as well as the service model, deployment model, and Federal Information Security Management Act of 2002 (FISMA) security level.[1]

DHS

Data Center Services: DHS is implementing a private cloud within two of its data centers to enhance sharing sensitive information across the department. The private cloud encompasses multiple services (DHS committed to OMB to move eight data center services to a cloud environment) to improve collaboration and information sharing within the department.

Employment Verification: This is a free service that workers can use to confirm employment eligibility in the United States. This service is to provide a mechanism by which DHS can validate identity, and control secure access to employment information.

Website Hosting: This service is intended to host DHS public-facing websites and offer an enterprise content delivery capability with 100 percent availability and provide a web content management capability to manage the content across all of the public-facing websites that reside within the public cloud offering.

[1] As required under FISMA, NIST guidance defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The three potential impact levels of a breach are: low (limited adverse effect), moderate (serious adverse effect), and high (catastrophic adverse effect).

Table 2: DHS Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Data Center Services			
E-mail	SaaS	Private	High
Production Infrastructure	IaaS	Private	Moderate
Development Test	IaaS	Private	Moderate
Workplace	IaaS	Private	Moderate
SharePoint	PaaS	Private	High
Project Server	PaaS	Private	High
Customer Relationship Management	PaaS	Private	High/Moderate
Business Intelligence	SaaS	Private	Moderate
Employment Verification	SaaS	Public	Moderate
Website Hosting	SaaS	Public	Moderate

Source: DHS.

Note: The service models are: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

GSA

Correspondence Tracking: This service is to allow the Federal Acquisition Service to track communication with Congress from when correspondence is received to the final processing of a response.

GSA's E-mail and Collaboration Solution: This cloud solution is to replace GSA's legacy e-mail system, and is to provide faster upgrades and improved customer service to approximately 17,000 users. In addition, this service is a critical component of GSA's mobile technology strategy.

IT Power Management Services: This new functionality manages the power settings for more than 17,000 GSA workstations and the Office of the Chief Information Officer's infrastructure servers. GSA estimates that it will reduce the carbon footprint by over 4.8 million carbon pounds a year by turning off computers every evening.

Table 3: GSA Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Correspondence Tracking	SaaS	Public	Moderate
GSA’s E-mail and Collaboration Solution	SaaS	Public	Moderate
IT Power Management Services	SaaS	Public	Moderate

Source: GSA.

HHS

Medwatch+: This service is to provide a web portal for reporting public safety information, as well as information by drug and biological product. This effort is comprised of three private cloud services: Safety Reporting, Device Adverse Reporting, and Drugs and Biologics Adverse Reporting. The first two services are already in cloud environments and the third is being migrated.

Grants Solutions: This suite of services is available to federal agencies and grantee/applicant organizations. These services cover 14 grant award processes for federal agencies and grantee/applicant organizations through GrantSolutions.gov.

Audit Resolution Tracking Management System: This “proof-of-concept” was designed to replace the Administration for Children and Families’ legacy Audit Resolution system. This service linked audit reports with the appropriate grantees and was expected to reduce hosting costs.

Table 4: HHS Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Medwatch+	PaaS	Private	Moderate
Grants Solutions	IaaS	Private	Moderate
Audit Resolution Tracking Management System	PaaS	Public	Moderate

Source: HHS.

SBA

Collaboration Services (Management and Technical Assistance Line of Business): This service is intended to encourage small business owners and small business lenders to take advantage of SBA programs, services, and loan options.

Human Resources (Performance Management): This new service is to provide tools for training and performance management while reducing annual infrastructure costs.

LAN/WAN, Offsite Vaulting: This is to provide online backup and recovery capabilities; and electronic vaulting for records retention.

Table 5: SBA Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Collaboration Services (Management and Technical Assistance Line of Business)	IaaS	Hybrid	Low
Human Resources (Performance Management)	SaaS	Private	Moderate
LAN/WAN, Offsite Vaulting	IaaS	Public	High

Source: SBA.

State

Electronic Library: This is to provide domestic and overseas agency staff with direct access to information in over 50 databases. The cloud solution is to add additional functionality including online, self-service resource check-in, check-out, and other library requests; regionalized and issue-driven electronic information portals; and an integrated electronic catalog with other online libraries.

Program Management: This service is to provide program managers of the Nonproliferation and Disarmament Fund access to agency data from any location.

Website Hosting: This is to provide access to keyword-searchable and downloadable government documents, unclassified publications, and databases regarding the history of State, diplomacy, and foreign relations.

Table 6: State Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Electronic Library	SaaS	Public	Low
Program Management	PaaS	Public	Low
Website Hosting	IaaS	Public	Low

Source: State.

Treasury

Business Process Management: This is to automate the Bureau of Engraving and Printing's processes for manufacturing, financial management, acquisition, and supply chains.

Document Management and Freedom of Information Act Case Management: This service is to provide the agency capabilities such as electronic capture, store, search/analyze, share, and document management.

Website Hosting: This service is to provide a flexible, scalable architecture for the department's main website and four additional websites.

Table 7: Treasury Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Business Process Management	SaaS	Private	Moderate
Document Management and FOIA Case Management	IaaS	Public	High
Website Hosting	IaaS	Public	Low

Source: Treasury.

USDA

Collaboration Services (USDA Connect): This service is to increase interagency interaction, productivity, and efficiency by providing tools such as Profiles, Wikis, Blogs, Communities, Activities, Files, and Bookmarks for over 107,000 USDA users.

Document Management and Correspondence Tracking: This is to eliminate redundancy and increased efficiency by consolidating over 20 systems to a single cloud-based customer relationship management environment to organize customer information and track correspondence throughout the agency.

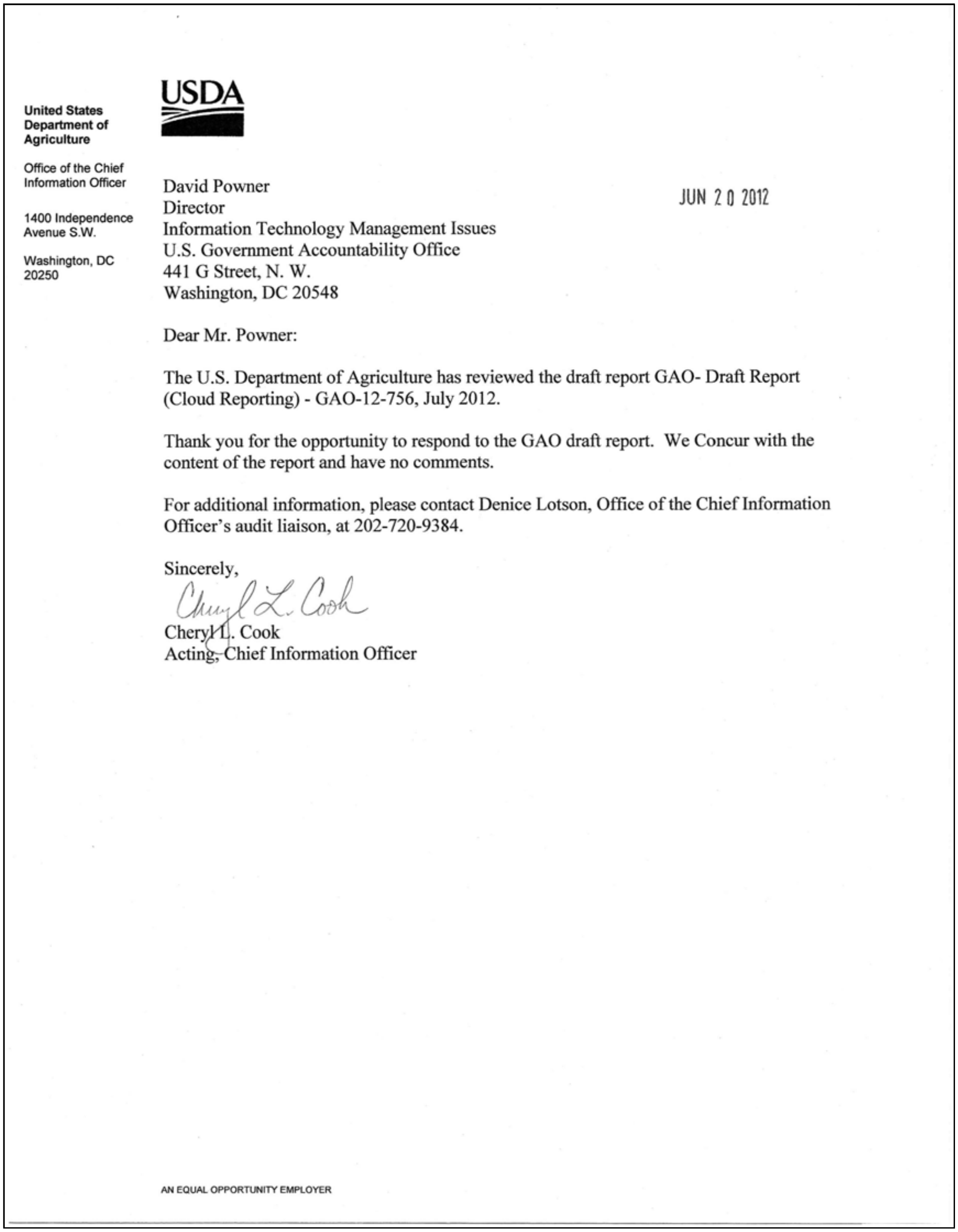
E-mail: This is to provide e-mail service for over 120,000 inboxes and enhanced agencywide collaboration through e-mail, instant messaging, web conferencing, and a global address list.

Table 8: USDA Service Model, Deployment Model, and FISMA Security Level by Service

Service	Service model	Deployment model	FISMA security level
Collaboration Services (USDA Connect)	SaaS	Private	Moderate
Document Management and Correspondence Tracking	PaaS	Public	Moderate
E-mail	SaaS	Public	Moderate

Source: USDA.

Appendix III: Comments from the Department of Agriculture



USDA

United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue S.W.

Washington, DC 20250

JUN 20 2012

David Powner
Director
Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, N. W.
Washington, DC 20548

Dear Mr. Powner:

The U.S. Department of Agriculture has reviewed the draft report GAO- Draft Report (Cloud Reporting) - GAO-12-756, July 2012.

Thank you for the opportunity to respond to the GAO draft report. We Concur with the content of the report and have no comments.

For additional information, please contact Denice Lotson, Office of the Chief Information Officer's audit liaison, at 202-720-9384.

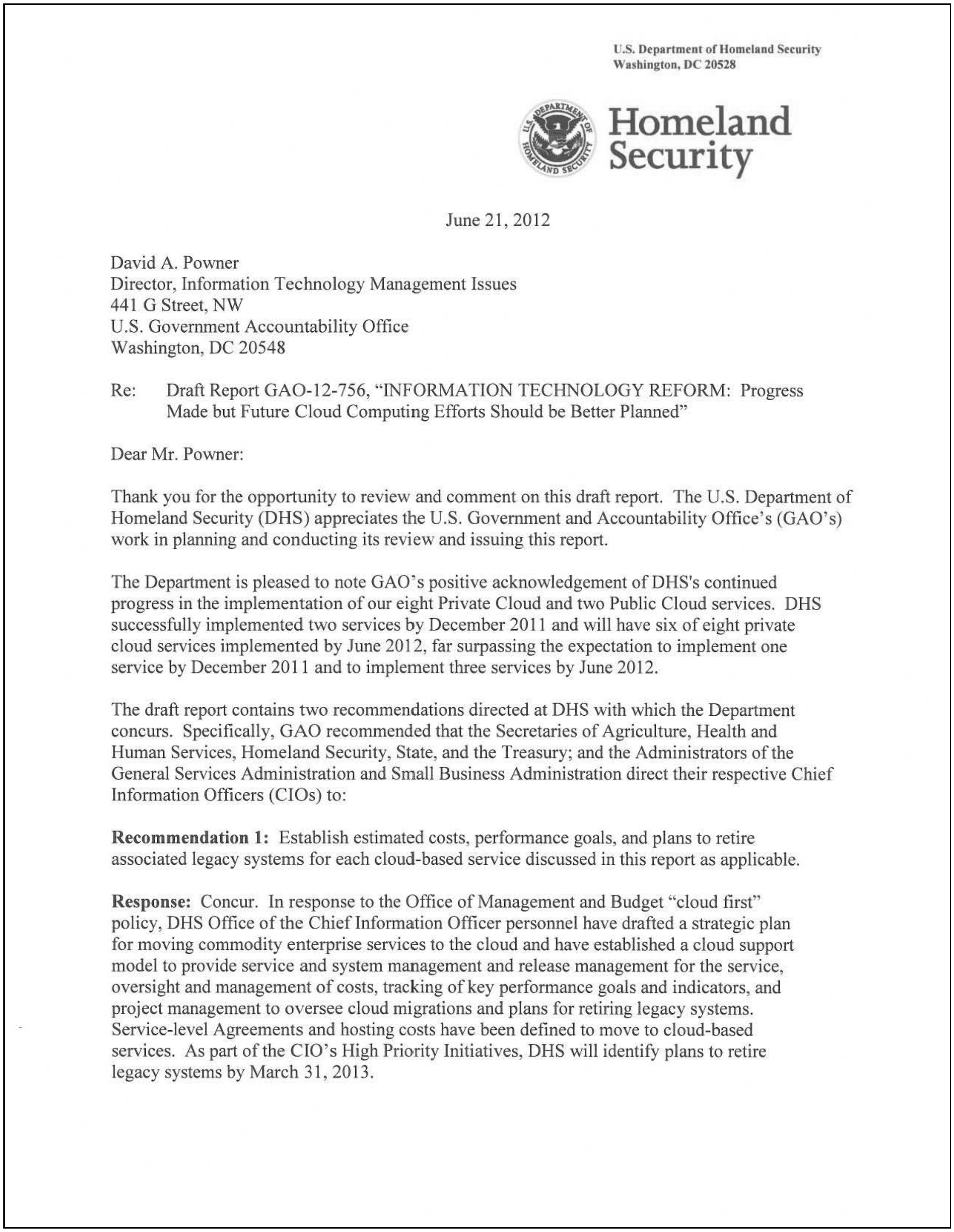
Sincerely,

Cheryl L. Cook

Cheryl L. Cook
Acting, Chief Information Officer

AN EQUAL OPPORTUNITY EMPLOYER

Appendix IV: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

June 21, 2012

David A. Powner
Director, Information Technology Management Issues
441 G Street, NW
U.S. Government Accountability Office
Washington, DC 20548

Re: Draft Report GAO-12-756, "INFORMATION TECHNOLOGY REFORM: Progress Made but Future Cloud Computing Efforts Should be Better Planned"

Dear Mr. Powner:

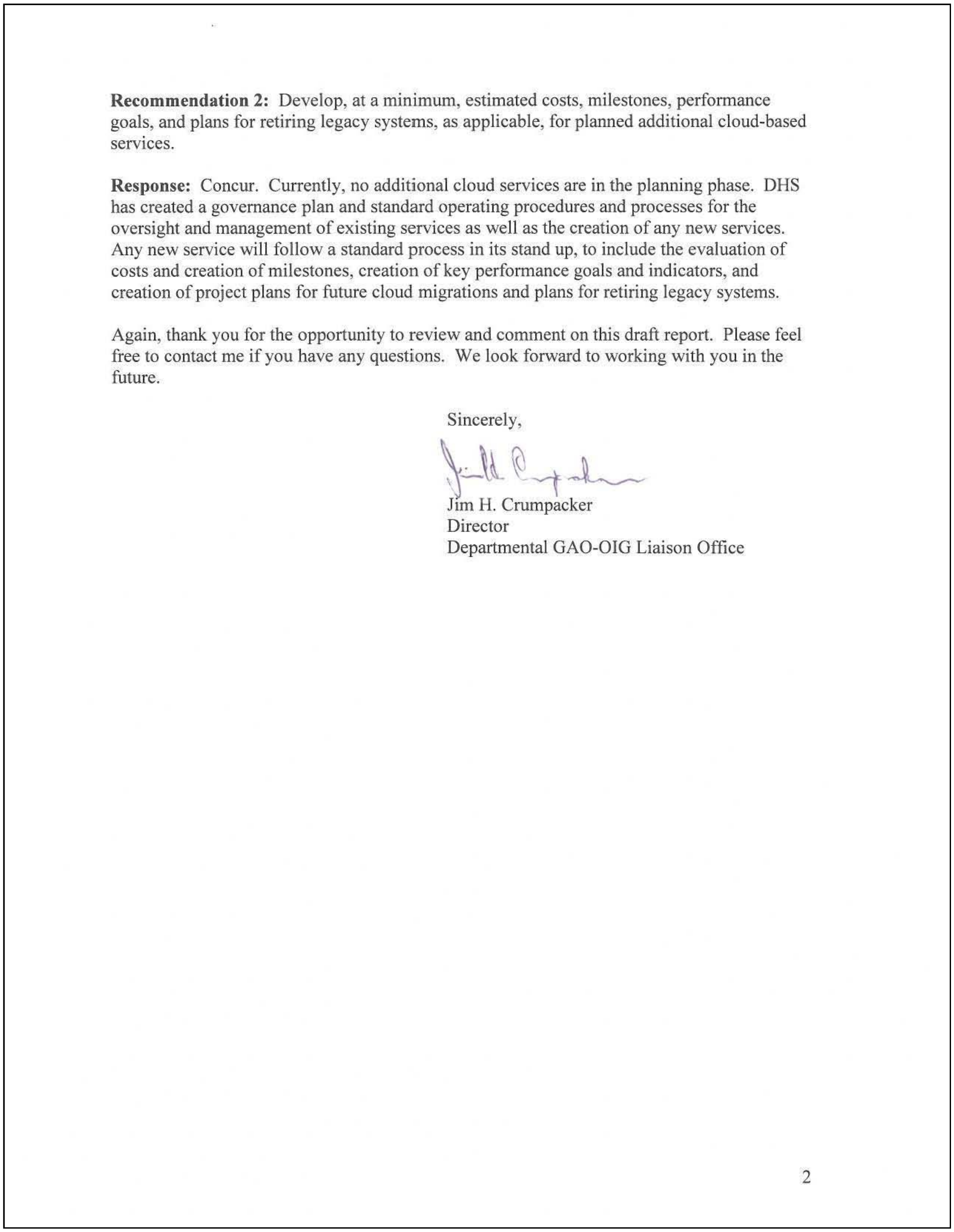
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government and Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive acknowledgement of DHS's continued progress in the implementation of our eight Private Cloud and two Public Cloud services. DHS successfully implemented two services by December 2011 and will have six of eight private cloud services implemented by June 2012, far surpassing the expectation to implement one service by December 2011 and to implement three services by June 2012.

The draft report contains two recommendations directed at DHS with which the Department concurs. Specifically, GAO recommended that the Secretaries of Agriculture, Health and Human Services, Homeland Security, State, and the Treasury; and the Administrators of the General Services Administration and Small Business Administration direct their respective Chief Information Officers (CIOs) to:

Recommendation 1: Establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed in this report as applicable.

Response: Concur. In response to the Office of Management and Budget "cloud first" policy, DHS Office of the Chief Information Officer personnel have drafted a strategic plan for moving commodity enterprise services to the cloud and have established a cloud support model to provide service and system management and release management for the service, oversight and management of costs, tracking of key performance goals and indicators, and project management to oversee cloud migrations and plans for retiring legacy systems. Service-level Agreements and hosting costs have been defined to move to cloud-based services. As part of the CIO's High Priority Initiatives, DHS will identify plans to retire legacy systems by March 31, 2013.



Recommendation 2: Develop, at a minimum, estimated costs, milestones, performance goals, and plans for retiring legacy systems, as applicable, for planned additional cloud-based services.

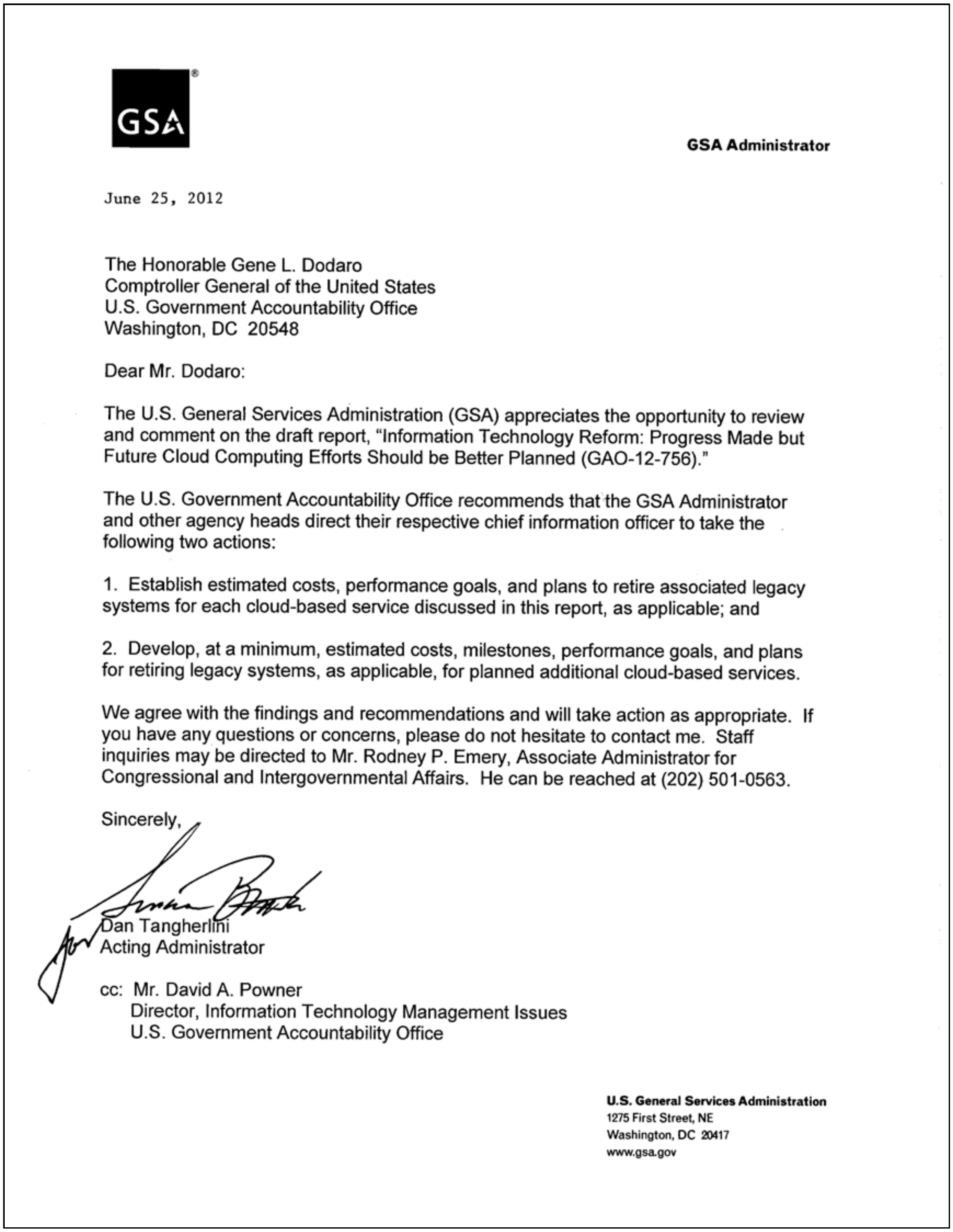
Response: Concur. Currently, no additional cloud services are in the planning phase. DHS has created a governance plan and standard operating procedures and processes for the oversight and management of existing services as well as the creation of any new services. Any new service will follow a standard process in its stand up, to include the evaluation of costs and creation of milestones, creation of key performance goals and indicators, and creation of project plans for future cloud migrations and plans for retiring legacy systems.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Appendix V: Comments from the General Services Administration



GSA Administrator

June 25, 2012

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned (GAO-12-756)."

The U.S. Government Accountability Office recommends that the GSA Administrator and other agency heads direct their respective chief information officer to take the following two actions:

1. Establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed in this report, as applicable; and

2. Develop, at a minimum, estimated costs, milestones, performance goals, and plans for retiring legacy systems, as applicable, for planned additional cloud-based services.

We agree with the findings and recommendations and will take action as appropriate. If you have any questions or concerns, please do not hesitate to contact me. Staff inquiries may be directed to Mr. Rodney P. Emery, Associate Administrator for Congressional and Intergovernmental Affairs. He can be reached at (202) 501-0563.

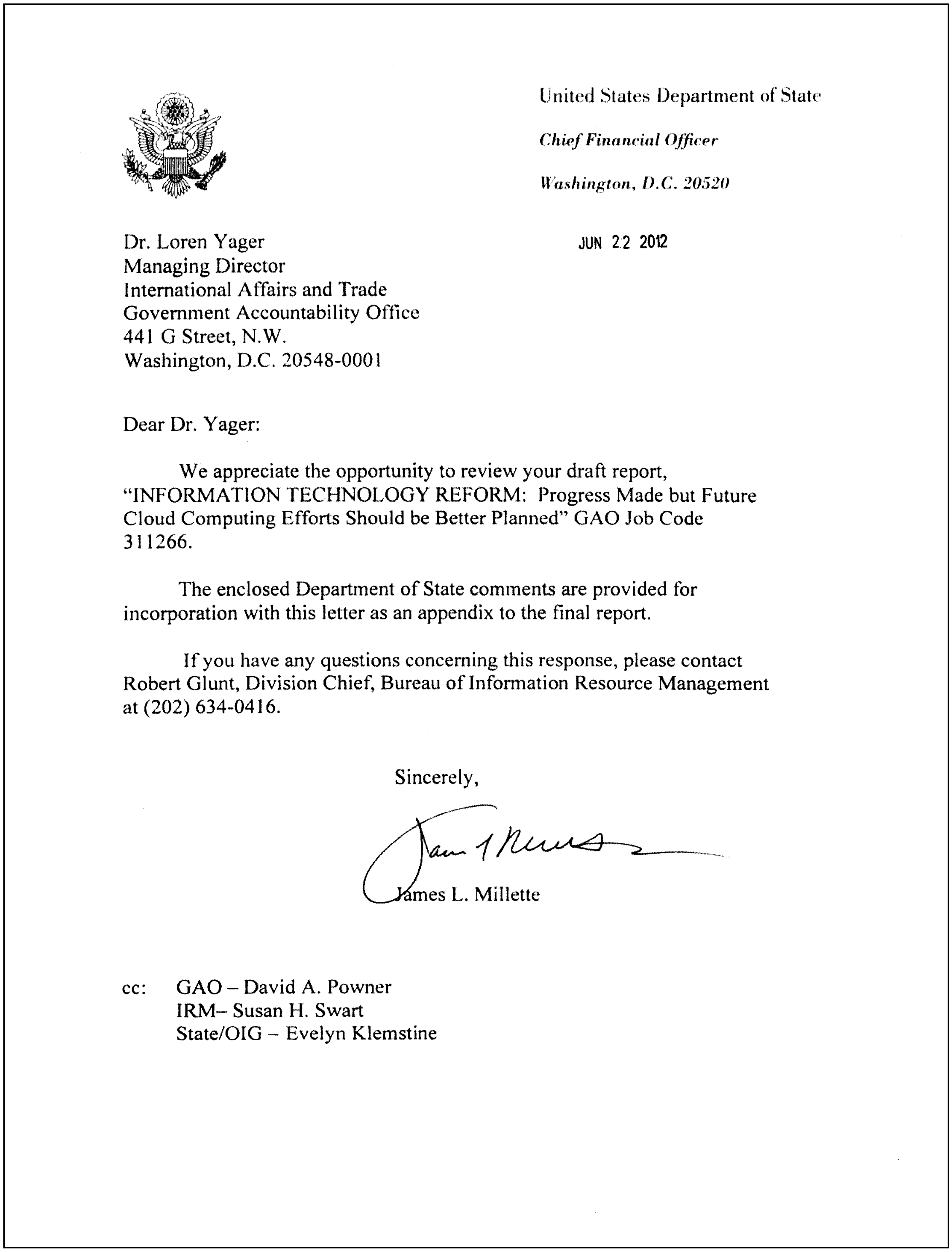
Sincerely,

Dan Tangherlini
Acting Administrator

cc: Mr. David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office

U.S. General Services Administration
1275 First Street, NE
Washington, DC 20417
www.gsa.gov

Appendix VI: Comments from the Department of State



United States Department of State

Chief Financial Officer

Washington, D.C. 20520

JUN 22 2012

Dr. Loren Yager
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "INFORMATION TECHNOLOGY REFORM: Progress Made but Future Cloud Computing Efforts Should be Better Planned" GAO Job Code 311266.

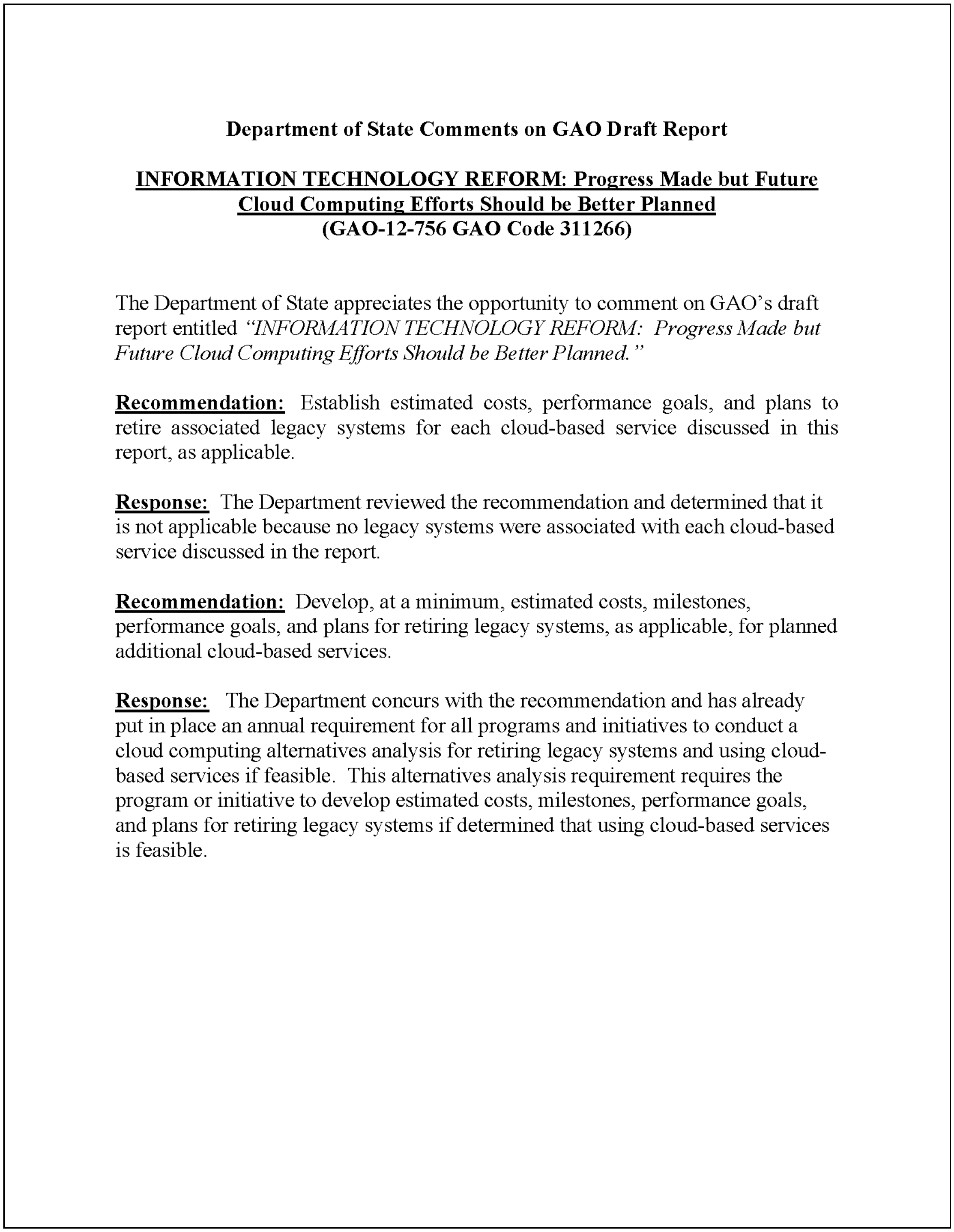
The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Robert Glunt, Division Chief, Bureau of Information Resource Management at (202) 634-0416.

Sincerely,

James L. Millette

cc: GAO – David A. Powner
IRM– Susan H. Swart
State/OIG – Evelyn Klemstine



Department of State Comments on GAO Draft Report

INFORMATION TECHNOLOGY REFORM: Progress Made but Future Cloud Computing Efforts Should be Better Planned
(GAO-12-756 GAO Code 311266)

The Department of State appreciates the opportunity to comment on GAO's draft report entitled *"INFORMATION TECHNOLOGY REFORM: Progress Made but Future Cloud Computing Efforts Should be Better Planned."*

Recommendation: Establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed in this report, as applicable.

Response: The Department reviewed the recommendation and determined that it is not applicable because no legacy systems were associated with each cloud-based service discussed in the report.

Recommendation: Develop, at a minimum, estimated costs, milestones, performance goals, and plans for retiring legacy systems, as applicable, for planned additional cloud-based services.

Response: The Department concurs with the recommendation and has already put in place an annual requirement for all programs and initiatives to conduct a cloud computing alternatives analysis for retiring legacy systems and using cloud-based services if feasible. This alternatives analysis requirement requires the program or initiative to develop estimated costs, milestones, performance goals, and plans for retiring legacy systems if determined that using cloud-based services is feasible.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff also made key contributions to the report: Deborah Davis (assistant director), Shannin O'Neill (assistant director), Nancy Glover, Sandra Kerr, Emily Longcore, Andrew Stavisky, and Kevin Walsh.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548