JULY 29, 2013

AUDIT REPORT

OFFICE OF AUDITS

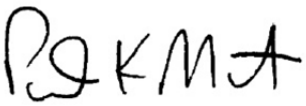
NASA'S PROGRESS IN ADOPTING CLOUD-COMPUTING TECHNOLOGIES

OFFICE OF INSPECTOR GENERAL

National Aeronautics and
Space Administration

REPORT NO. IG-13-021 (ASSIGNMENT NO. A-12-022-00)

Final report released by:



Paul K. Martin
Inspector General

Acronyms

CIO	Chief Information Officer
CSSO	Computer Services Service Center
FedRAMP	Federal Risk and Authorization Management Program
GSA	General Services Administration
IT	Information Technology
JPL	Jet Propulsion Laboratory
NIST	National Institute for Standards and Technology
NSSC	National Shared Service Center
OCIO	Office of Chief Information Officer
OMB	Office of Management and Budget

OVERVIEW

NASA'S PROGRESS IN ADOPTING CLOUD-COMPUTING TECHNOLOGIES

The Issue

NASA spends about $1.5 billion annually on its portfolio of information technology (IT) assets, which includes more than 550 information systems that control spacecraft, collect and process scientific data, provide security for IT infrastructure, and enable Agency personnel to collaborate with colleagues around the world. In addition, hundreds of thousands of individuals, including NASA employees, contractors, members of academia, and the general public, use these IT systems daily.

The adoption of cloud-computing technologies has the potential to improve IT service delivery and reduce the costs associated with managing NASA's diverse IT portfolio. Specifically, cloud computing offers the potential for significant cost savings through faster deployment of computing resources, a decreased need to buy hardware or build data centers, and enhanced collaboration capabilities.

To accelerate the Federal Government's use of cloud-computing strategies, the Office of Management and Budget (OMB) requires agencies to adopt a "Cloud First" policy when contemplating IT purchases and evaluate secure, reliable, and cost-effective cloud-computing alternatives when making new IT investments.[1] In addition, OMB required agencies to move one existing IT service to the cloud by December 2011 and two more by June 2012.

To help Federal agencies meet Cloud First requirements, the General Services Administration, in collaboration with several other agencies, established the Federal Risk Authorization Management Program (FedRAMP). FedRAMP helps agencies adopt cloud-computing technologies by (1) ensuring that cloud providers have adequate IT security, (2) eliminating duplication of effort and reducing risk management costs, and (3) enabling rapid and cost-effective purchasing of cloud-computing services. By June 2014, agencies are required to utilize only FedRAMP-approved cloud service providers.

When transitioning to a cloud-computing model, agencies may adopt a private cloud strategy in which they operate their own data centers or purchase cloud services from public providers like Amazon or Microsoft. While the private cloud alternative enables agencies to manage their critical IT services and control access to sensitive data directly,

[1] Office of the U.S. Federal Chief Information Officer, "25 Point Implementation Plan to Reform Federal Information Technology Management," December 2010.

these benefits come at the high cost of owning and operating data centers. Conversely, the public cloud alternative frees organizations from the expense of data center ownership but requires that they effectively manage contractor performance to ensure key business and IT security requirements are met.

NASA was a pioneer in cloud computing having established its own private cloud-computing data center called Nebula in 2009 at the Ames Research Center (Ames). Nebula provided high-capacity computing and data storage services to NASA Centers, Mission Directorates, and external customers. In 2012, NASA shut down Nebula based on the results of a 5-month test that benchmarked Nebula's capabilities against those of Amazon and Microsoft. The test found that public clouds were more reliable and cost effective and offered much greater computing capacity and better IT support services than Nebula.

Effectively managing the delivery of public cloud-computing services requires agencies to develop contracts that address business and security risks as well as properly defining and providing a mechanism to monitor agency and cloud provider responsibilities. In addition, agencies must have strong IT governance practices in place, including organizational control of and oversight over policies, procedures, and standards for IT service acquisition and for monitoring the use of IT services. Because of the wide availability and ease of purchasing services from public cloud providers, a lack of organizational control over the acquisition of these services can create problems. For example, if cloud-computing services are acquired without proper approvals and oversight, vulnerable systems and sensitive information may be placed in the cloud environment, legal and privacy requirements may go unmet, and costs may quickly accrue to unacceptable levels.

Our overall audit objective was to evaluate the efficacy of NASA's efforts to adopt cloud-computing technologies. To do this we evaluated whether NASA had implemented

- an Agency-wide governance model with processes to manage life-cycle activities for transitioning to a cloud-computing model for delivery of IT services and

- practices to evaluate security and risks within the cloud-computing model and implement appropriate control mechanisms that reduce these risks to acceptable levels.

Details of the audit's scope and methodology can be found in Appendix A.

Results

We found that weaknesses in NASA's IT governance and risk management practices have impeded the Agency from fully realizing the benefits of cloud computing and potentially put NASA systems and data stored in the cloud at risk. For example, several NASA Centers moved Agency systems and data into public clouds without the knowledge or consent of the Agency's Office of the Chief Information Officer (OCIO). Moreover, on five occasions, NASA acquired cloud-computing services using contracts that failed to fully address the business and IT security risks unique to the cloud environment. Finally, one of the two moderate-impact systems NASA moved to a public cloud operated for 2 years without authorization, a security or contingency plan, or a test of the system's security controls.[2] This occurred because the Agency OCIO lacked proper oversight authority, was slow to establish a contract that mitigated risks unique to cloud computing, and did not implement measures to ensure cloud providers met Agency IT security requirements.

In December 2012, the Agency OCIO developed a contract for acquiring services from public cloud providers that addresses key business and IT security risks and meets FedRAMP requirements. However, the Agency does not currently require that Centers use the contract when acquiring cloud services or incorporate similar terms in the contract they use. Finally, we found that NASA satisfied OMB's requirement to move several existing IT services to the cloud by June 2012.

At the time of our audit, NASA spent less than 1 percent (about $10 million) of its $1.5 billion annual IT budget on cloud computing. However, NASA projects that within 5 years up to 75 percent of new IT programs could begin in the cloud and nearly 100 percent of the Agency's public data could be moved to the cloud. Moreover, as legacy systems are modernized, up to 40 percent of them could be moved to the cloud. As NASA moves more of its systems and data to the cloud, it is imperative that the Agency strengthen its governance and risk management practices to safeguard its data while effectively spending its IT funds.

NASA's Governance of Its Cloud-Computing Efforts Needs Strengthening. Having an enterprise-wide inventory of cloud-computing services and providers is a best practice and helps organizations ensure they do not use unapproved or unsecured services. We found that the Agency OCIO was not aware of all the cloud services NASA organizations had acquired or which service providers they used. In addition, only 3 of 15 Center and Mission Directorate Chief Information Officers we surveyed stated that coordination with the Agency OCIO was necessary before moving NASA systems and data to public clouds. This occurred because NASA did not effectively communicate to its Centers their responsibilities for coordinating with the Agency OCIO when acquiring cloud-

[2] According to the National Institute of Standards and Technology, in a moderate-impact system, the loss of confidentiality, integrity, or availability could have serious adverse effects on an organization's operations, assets, or individuals. In a high-impact system, such a loss could be expected to have severe or catastrophic effects.

computing services. We also found that the Agency OCIO was slow to establish an enterprise-wide cloud-computing strategy or process for evaluating which NASA systems and data can be economically and securely stored in a public cloud. Moving systems and data into a public cloud without first developing such a plan increases the risk that public funds may be misspent and puts information resources at risk of compromise.

NASA's Risk Management Practices for Acquiring and Securing Public Cloud-Computing Services Were Ineffective. Assessing and managing risk when putting a Federal agency's systems and data into a public cloud poses a challenge because the computing environment is under the control of the cloud provider rather than the agency. Thus, effective risk mitigation requires developing contracts that address how contractor performance will be managed and how Federal privacy, IT security, and record management requirements will be met. We reviewed five NASA contracts for the acquisition of cloud-computing services and found that none came close to meeting recommended best practices for ensuring data security. Rather, in four cases NASA organizations accepted the cloud providers' standard contracts that did not impose performance metrics or address Federal privacy, IT security, or record management requirements. For the fifth contract, NASA developed its own contract with a third party IT services firm to ensure that Federal IT security requirements were met. However, we found that the negotiated contract also failed to include best practices for ensuring data security or for effectively managing contractor performance. As a result, the NASA systems and data covered by these five contracts are at an increased risk of compromise.

One of NASA's Two Moderate-Impact Cloud Services Failed to Meet Key IT Security Requirements. We reviewed system security and contingency plans and annual security control tests associated with the two moderate-impact cloud services NASA has deployed to public clouds to determine whether they met Federal and Agency IT security requirements. We found that the cloud service used to deliver Internet content for more than 100 NASA internal and public-facing websites had been operating for more than 2 years without written authorization or system security or contingency plans. More troubling, the required annual test of the service's security controls had not been performed to determine whether the controls were implemented correctly, operating as intended, and producing the desired result of securing the cloud service and its data. A breach of this moderate-impact cloud service could result in a serious disruption to NASA operations.

NASA's West Prime Contract Complies with FedRAMP Standards but Agency Organizations Are Not Required to Leverage this Contract to Obtain Cloud Services. In December 2012, the Agency OCIO entered into an IT services contract with InfoZen, Inc. to address the business and IT security risks unique to public cloud-computing environments (WestPrime contract). We found that this contract adequately outlines the respective roles and responsibilities of the Agency and cloud service providers and contains standards governing how contractor performance will be measured, reported, and enforced. Furthermore, the contract addresses Federal privacy, data retention, and destruction requirements as well as incident detection and handling

practices. However, NASA has not mandated that Centers use the WestPrime contract when acquiring cloud services or incorporate similar terms in the contract they use.

Management Action

While the adoption of cloud-computing technologies at NASA has the potential to improve IT service delivery, enhance collaboration, and reduce costs associated with managing the Agency's diverse portfolio of IT assets, fully realizing these benefits will require strengthening the Agency's IT governance and risk management practices. Accordingly, we recommend that NASA's Chief Information Officer (CIO) establish a cloud-computing program management office authorized to promulgate an Agency cloud-computing strategy; define related standards; and approve, coordinate, and oversee Agency-wide acquisition and deployment of cloud-computing services. In addition, we recommend the Agency CIO direct all Center and Mission Directorate CIOs to review FedRAMP policies and take actions necessary to meet policy requirements, require NASA organizations to use WestPrime or a contract with similar FedRAMP-compliant terms when acquiring cloud services, and establish an oversight function to ensure that moderate- and high-impact NASA systems and data are not moved to public clouds unless Federal and Agency IT security requirements are met. Finally, to remedy IT security deficiencies associated with the moderate-impact cloud service currently operating without authorization, we recommend that the system owner direct the service provider to immediately develop system and contingency plans that comply with National Institute of Standards and Technology standards and perform a test of the system's security controls.

In response to a draft of this report, NASA's CIO concurred with our recommendations and proposed corrective actions, subject to the availability of funds, to improve NASA's IT governance and risk management practices. We consider the Agency CIO's planned actions responsive and we will close the recommendations upon verification that the Agency has completed them. Management's response is reprinted in Appendix B.

CONTENTS

INTRODUCTION

Background

According to the National Institute of Standards and Technology (NIST), cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, such as computer servers, storage, software applications, and web services, that can be provisioned and released with minimal management effort or service provider interactions. In other words, in a cloud environment, information technology (IT) resources are available to users as needed using a pay-as-you-go business model.

NASA uses cloud computing to accommodate a number of functions such as large-scale computational services to support the Agency's science programs and storage of large data sets associated with high-resolution mapping of planetary surfaces, as well as for more routine services like website hosting and document storage. In contrast to the traditional data center model that requires a significant initial investment in IT hardware and does not support automatic provisioning of IT resources, cloud computing allows NASA scientists and engineers to use only the resources needed to complete a particular project or function and to release those resources for use by others when that need ends. Consequently, cloud computing offers the potential for significant cost savings through more efficient utilization of computing resources.

Cloud-computing environments share five essential characteristics.

- *On-demand self-service*: A consumer can unilaterally and automatically provision computing resources such as processing, data storage, and network bandwidth.

- *Broad network access*: Computing resources are available over the Internet or internal networks and accessed through web browsers on a variety of devices, including smart phones, tablets, laptops, and workstations.

- *Resource pooling*: Computing resources are pooled to serve multiple consumers. Resources may be assigned and reassigned according to consumer demand and the consumer typically has no control over or knowledge of the location of the provided resources.

- *Rapid elasticity*: Resources can be provisioned elastically and released rapidly to scale up or down commensurate with demand so that computer processing, data storage, and network bandwidth appear unlimited to the consumer.

- *Measured service*: Cloud systems automatically control and optimize resource use through a metering technology matched to the resource consumed. Thus, resource usage can be monitored, controlled, and reported providing transparency over the type and amount of services used.

In addition, cloud-computing operations generally utilize three service and four deployment models.

Service Models

- *Infrastructure as a Service*: Capability to provision computer processing, data storage, and network bandwidth to enable the customer to deploy and run software, including operating systems and applications.

- *Platform as a Service*: Capability to deploy onto the cloud infrastructure customer-created or -acquired applications created using programming languages and tools supported by the provider.

- *Software as a Service*: Capability to use the provider's applications that run on the cloud infrastructure and are accessible to the client using an interface such as a web browser for e-mail.

Deployment Models

- *Private Cloud*:
  - operated solely for an organization
  - managed by the organization or a third party
  - may exist on or off organization's premises
- *Public Cloud*:
  - made available to the general public or a large industry group
  - owned by an organization that sells cloud services, such as Amazon, Microsoft, or Google
- *Community Cloud*:
  - shared by several organizations
  - supports a specific community with a shared mission or interest
  - managed by one of the organizations or a third party

  - may reside on or off the organizations' premises

- *Hybrid Cloud*:

  - composed of two or more private, community, or public clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)[3]

Nebula: NASA's Private Cloud-Computing Initiative. NASA was a pioneer in the development of private cloud-computing technologies. In 2009, the Agency established Nebula, a private cloud at the Ames Research Center (Ames). Until it was decommissioned in April 2012, Nebula provided computation and storage services to 73 NASA projects and fee-based IT services to the General Services Administration (GSA) and Microsoft.[4] Most Nebula projects were managed by Ames or the Goddard Space Flight Center (Goddard) and conducted as tests to assess the performance and suitability of storing scientific and business data in a cloud environment.

Nebula was housed at Ames in a standard sized shipping container (figure 1). As configured, this shipping container could accommodate approximately 15,000 central processing units or up to 15 petabytes of data.[5] For comparison, a contemporary public cloud-computing data center contains up to 376,000 central processing unit cores or more than 25 times the computer processing capacity of Nebula (figure 2).

[3] Cloud bursting is when a computer system in an organization's data center accesses additional resources from a public cloud to meet a surge in user demand.

[4] Among other activities, Nebula hosted GSA's "USASpending.gov" websites.

[5] One petabyte is equal to 1 million billion bytes.

Figure 1: Nebula: NASA's Cloud-Computing Data Center

Source: NASA.

Figure 2: Amazon.com Cloud-Computing Data Center

Source: Amazon.com.

NASA Partners with Private Sector and Distributes Free Software for Managing Private Clouds. In July 2010, NASA and Rackspace, a publicly held, cloud-computing company, launched OpenStack – an open-source software project whose goal is to provide a free alternative to buying services from public cloud-computing providers or paying expensive license fees for commercial cloud software.[6] OpenStack provides an Infrastructure as a Service capability by combining two technologies: compute, a NASA technology that provisions virtual machines at massive scale, and object storage, a Rackspace technology that reliably stores billions of objects distributed across standard hardware.[7] As part of the OpenStack project, NASA and Rackspace waived their intellectual property rights and released the software under an Apache 2.0 or "open-source" software license that allows anyone to use, modify, and redistribute the software freely.[8] NASA's then Chief Technology Officer believed that releasing Agency software for development by the public would increase product quality, reduce development costs, and remove barriers to public-private collaboration. More than 150 companies have joined the OpenStack project, including Intel, IBM, Dell, Hewlett-Packard, and Yahoo. The OpenStack community operates around a 6-month software release cycle with frequent development milestones. Since July 2010, the community has issued seven major releases of the OpenStack software program.

NASA Conducts Assessment of Nebula and Finds that Public Clouds Are More Reliable and Cost Effective. From July to November 2011, the Science Mission Directorate benchmarked Nebula's cloud-computing capabilities against those of Amazon and Microsoft. The objective was to determine which service offered the most stable and cost effective cloud-computing platform with sufficient scale and support services to meet the computational needs of NASA's engineering and science communities.[9] The tests found that the public clouds had matured to be more reliable and cost effective and offered much greater capacity and better IT support than Nebula. Thus, after investing $19.7 million, NASA suspended funding for Nebula in 2012 and shifted its cloud strategy to the purchase of cloud services from public providers. According to the Agency OCIO, NASA repurposed Nebula's computer hardware to meet other computing needs at the Agency and the cloud-computing skills developed by NASA staff during the Nebula project have aided the Agency's adoption of public cloud services.

NASA's Use of Public Cloud-Computing Services. We surveyed all NASA Centers, Mission Directorates, Headquarters, and the NASA Shared Services Center (NSSC) to develop an Agency-wide inventory of public cloud services used at NASA. As of August

[6] With open-source software, the copyright holder makes the source code available free of charge and provides the rights to study, change, and distribute the software to anyone and for any purpose.

[7] A virtual machine is a software implementation of a computer that executes programs like a physical computer.

[8] Apache 2.0 is the most widely used type of open-source software license.

[9] The tests focused on computer processing capabilities and did not assess the data storage services of the participants.

2012, Headquarters, the Jet Propulsion Laboratory (JPL), Johnson Space Center (Johnson), Marshall Space Flight Center (Marshall), and the NSSC were purchasing cloud-computing services either directly from public cloud providers or through cloud brokers using either existing contracts or, for services costing less than $3,000, with a NASA purchase card.[10] In addition, two other Centers are planning to acquire cloud services in the future. The types of cloud services acquired include website hosting, computation, and data storage. For example NASA's main public website (www.nasa.gov), which receives more than 140 million visits per year, is hosted by a public cloud (figure 3).

Figure 3: NASA's Public Internet Portal

Source: NASA portal at www.nasa.gov.

Office of Chief Information Officer. As part of its effort to implement Agency-wide web services, NASA's OCIO entered into a contract with eTouch Federal Systems (eTouch). Over time, NASA revised this contract to require eTouch to provide enhanced IT security measures to meet Federal IT security requirements. These services include incident detection, contingency planning, and testing of cloud providers' security controls. eTouch has worked primarily with the Agency OCIO; however, other NASA organizations may purchase eTouch's IT services for their own projects.

[10] Brokers are parties that provide services to cloud consumers, such as enhanced security, identity management, and performance reporting, that are typically not included in the cloud provider's service contract.

Until December 2012, eTouch managed the NASA Portal, which provides a secure application and hosting environment for Agency applications, content, and utilities. The NASA Portal has two parts: an internal portal for applications accessible only to internal NASA users and the external portal accessible to the public and NASA partners. Overall, the NASA Portal includes approximately 140 websites. In December 2012, NASA awarded management of its portal to InfoZen, a Maryland-based IT services firm. The total cost of InfoZen's 5-year contract to provide NASA cloud-computing services is $40 million.

Jet Propulsion Laboratory. JPL uses Amazon to host its "Be a Martian" educational website (http://beamartian.jpl.nasa.gov/welcome), which enables individuals to establish an account as a "Martian citizen" and explore the planet. JPL also uses cloud services to provide storage and increased computing capacity to its IT group.

Johnson Space Center. Johnson is using public cloud technology to host an IT innovation site that enables NASA employees to collaborate on IT issues such as improving Center practices for software upgrades. In addition, Johnson uses a public cloud to provide video production and editing for broadcasting NASA activities to the public, such as the day-to-day activities on the International Space Station. Johnson's Information Resources Directorate also plans to conduct two small, short-term projects to validate cost models, technical approach, and performance of cloud-based services. One pilot will move a noncritical internal application to the cloud and the second will test the cloud as a storage system for data backups.

Marshall Space Flight Center. Marshall is utilizing the cloud for a variety of mission-related services involving experiments for the International Space Station; environmental monitoring, impact, and response data; and hosting a website relating to the design, manufacture, and operation of more reliable and cost-effective spacecraft.

NASA Shared Services Center. NSSC provides financial management, human resources, IT, and procurement services to NASA employees. NSSC contracted with a cloud service provider to provide a suite of applications for employees to find information on a website rather than contacting NSSC's call center. By using the cloud service provider, NSSC is able to reduce call center costs by increasing customer's use of its websites.

NASA Continues to Invest in Private Cloud-Computing Initiatives. In July 2012, NASA awarded a $1.5 million contract for a containerized cloud-computing data center at Goddard. This private cloud provides computing and storage capabilities for the Agency's Science Mission Directorate.

"Cloud First" and Federal Risk and Authorization Management Program (FedRAMP). As part of its "Cloud First" initiative, the Office of Management and Budget (OMB) requires agencies to evaluate secure, reliable, and cost-effective cloud-computing alternatives when making new IT investments. In addition, agencies were required to move one existing IT service to the cloud by December 2011 and two additional services to the cloud by June 2012.

FedRAMP is a government wide cloud-computing program designed to help agencies meet the requirements of OMB's Cloud First initiative. FedRAMP was developed in collaboration with NIST, GSA, and the Departments of Defense and Homeland Security. There are five major participants in the FedRAMP process:

- *Federal agency customer*: any Federal agency that has a requirement for cloud technology.

- *Cloud service provider*: a private (e.g., Amazon, Microsoft, etc.) or public (e.g., a Federal agency offering services to other federal agencies) entity willing and able to fulfill customer requirements.

- *Joint Authorization Board*: a panel composed of representatives from GSA and the Departments of Defense and Homeland Security that reviews the security package submitted by the cloud service provider and grants the service provider provisional authority to operate.

- *Third party assessor*: an entity such as a public accounting firm that validates the quality and compliance of the cloud service provider's security program.

- *FedRAMP Program Management Office*: a GSA group that provides operational management of the FedRAMP process and ensures effective communication among all stakeholders.

FedRAMP helps agencies adopt cloud-computing technologies by (1) ensuring offered services have adequate IT security, (2) eliminating duplication of effort and reducing risk management costs, and (3) enabling rapid and cost-effective purchase of services. Beginning June 2014, Federal agencies may only obtain cloud-computing services from providers that have been authorized through the FedRAMP process.

Objectives

Our overall audit objective was to evaluate the efficacy of NASA's efforts to adopt cloud-computing technologies. To do this, we evaluated whether NASA had implemented

- an Agency-wide governance model with processes to manage life-cycle activities for transitioning to a cloud-computing model for delivery of IT services and

- practices to evaluate IT security risks within the cloud-computing model and appropriate control mechanisms for reducing identified risks.

See Appendix A for details of the audit's scope and methodology, our review of internal controls, and a list of prior coverage.

NASA NEEDS TO IMPROVE ITS IT GOVERNANCE AND RISK MANAGEMENT PRACTICES TO FULLY REALIZE THE BENEFITS OF CLOUD COMPUTING

We found that weaknesses in NASA's IT governance and risk management practices impeded the Agency from fully realizing the benefits of cloud computing and potentially placed at risk its information stored in the cloud. For example, Centers moved Agency systems and data into public clouds without the knowledge or approval of NASA's OCIO. Moreover, on five occasions NASA acquired cloud-computing services using contracts that failed to address or mitigate key business and IT security risks. In addition, one of the two moderate-impact systems NASA moved to the public cloud operated for years without authorization, security or contingency plans, or a test of the system's security controls. This occurred because the Agency OCIO lacked proper oversight authority, was slow to establish a contract that mitigated risks unique to cloud computing, and did not implement measures to ensure cloud providers met IT security requirements before putting Agency systems and data into public clouds. In December 2012, NASA signed a contract with a vendor to acquire cloud-computing services that address key business and IT security risks. However, the Agency currently does not require NASA Centers, to utilize this contract or to incorporate similar FedRAMP-compliant terms in contracts when acquiring cloud services. We also found that NASA satisfied the requirement of OMB's Cloud-First initiative by moving several existing IT services from data centers to the cloud.

NASA projects that within 5 years up to 75 percent of new IT programs will begin in the cloud and nearly 100 percent of the Agency's public data could be stored in the cloud. Moreover, as legacy systems are modernized, up to 40 percent of them could be moved to the cloud. As the Agency moves more of its systems and data to the cloud, it is imperative that NASA strengthen its governance and risk management practices to safeguard its data while effectively spending its IT funds.

NASA's Governance of Cloud Computing Needs Strengthening

According to ISACA, having an enterprise-wide inventory of cloud-computing services and providers is a best practice that helps organizations ensure they do not use unapproved or unsecured services.[11] In addition, NASA will need a complete inventory

[11] Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only to reflect the broad range of IT governance professionals it serves. ISACA is a global organization engaged in the development and adoption of widely accepted, industry-leading practices for information systems.

of its cloud service providers to ensure it meets GSA's requirement that Federal agencies utilize only FedRAMP-approved providers by June 2014.

As part of our audit, we asked the Agency OCIO for a NASA-wide inventory of deployed cloud services and associated service providers. We also surveyed the NASA Centers, Mission Directorates, Headquarters, and NSSC to identify their deployed cloud services and related service providers. We found that the Agency OCIO was unaware of two of the eight companies providing cloud services to NASA organizations and that two Centers had implemented cloud services. In addition, only 3 of 15 NASA organizations surveyed indicated that coordination with the Agency OCIO was required before moving systems and data into public clouds. We attribute this to NASA's failure to effectively communicate to Centers' their responsibility for coordinating with the Agency OCIO when acquiring cloud-computing services.

We also found that the Agency OCIO was slow to establish an Agency cloud-computing strategy or guidelines for evaluating which NASA systems and data are suitable for transfer to a public cloud. Although such efforts are under development and include a framework for Agency programs to securely and efficiently use public cloud environments, NASA does not expect these initiatives to be fully developed until fiscal year 2014. In the meantime, moving systems and data into a public cloud without a plan or effective oversight can result in deployment of services that fail to meet key business or IT security requirements, which in turn can lead to loss of availability, integrity, and confidentiality of systems and data.

NASA's Risk Management Practices for Acquiring and Securing Public Cloud-Computing Services were Ineffective

According to NIST, assessing and managing the risks of transferring systems and data to a public cloud poses a challenge because the computing environment is under the control of the cloud provider. Accordingly, effective risk mitigation in this context requires developing contracts that address business and security risks unique to cloud-computing environments. Specifically, contracts with cloud service providers should contain clauses explaining how contractor performance will be measured, reported, and enforced and specify how Federal privacy, litigation discovery, and data retention and destruction requirements will be met. In addition, contracts should prescribe how cloud providers will perform such important IT security activities as incident detection and require that providers' IT security programs periodically be evaluated and certified by an independent third party. Finally, attention to the roles and responsibilities of the Agency, the cloud provider, and the cloud broker is also required to drive contractor performance and ensure Agency systems and data are adequately secured.

Specifications for public cloud services are generally called service agreements or service contracts. A service contract defines the terms and conditions for access and use of the services offered by the cloud provider and establishes the period of service, conditions for

termination, and disposition of data (e.g., preservation period) upon contract termination. Typically, the complete terms and conditions for a cloud service contract are contained in multiple documents, including a service level agreement and privacy and acceptable use policies.

NIST has identified two types of cloud-computing service contracts: predefined, nonnegotiable contracts and negotiated contracts. Under a predefined contract, the contract terms are prescribed by the cloud provider. As such, these contracts typically do not impose requirements on the provider beyond meeting a base level of service and availability. Nor do they address Federal IT security, privacy, data production, or retention and destruction requirements. Furthermore, the provider is often empowered to modify the contract unilaterally without notifying the customer. Negotiated service contracts are more like traditional outsourcing contracts for IT services. In these contracts, terms can be tailored to address an agency's requirements for tracking and reporting service effectiveness, prescribe technical controls such as incident detection and handling, require compliance with laws and regulations and the use of validated products meeting national or international standards, and include data ownership rights.

As a best practice, the Federal Chief Information Officer (CIO) and Chief Acquisition Officer Councils recommend that contracts for cloud services clearly define how performance is guaranteed (such as response time, resolution or mitigation time, and availability) and require providers to monitor their service levels and provide timely reporting of failures to meet service levels. Moreover, contracts should include enforcement mechanisms that prescribe penalties when service levels are not met.

To determine whether the Agency had implemented effective risk mitigation measures, we reviewed NASA's contracts with providers of public cloud-computing services. Specifically, we examined whether the contracts met best practices for acquiring cloud services as recommended by the Federal CIO and Chief Acquisition Officer Councils, as well as practices identified in FedRAMP.[12] For example, we evaluated if the contracts specified the roles and responsibilities of the parties and how contractor performance would be measured, reported, and enforced. We also assessed whether the contracts addressed Federal privacy, discovery, and data retention and destruction requirements. Finally, we determined if the service providers or brokers adequately addressed key IT security measures, such as incident detection and handling practices, and whether the providers' IT security programs had been independently evaluated and certified. The results of our review are summarized in Table 1.

For the five NASA cloud-computing contracts we reviewed, three were for cloud services categorized as low-impact services and two were for moderate-impact services. NASA accepted the cloud providers' standard service contract for the three low-impact and one of the moderate-impact cloud services. For the other moderate-impact cloud service, which hosts more than 100 internal and external Agency websites, NASA negotiated a

[12] FedRAMP, "Creating Effective Cloud-Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service," (February 2012).

contract with eTouch, a cloud-computing broker, to manage service delivery and help ensure IT security and privacy requirements were met.

As the table below indicates, none of the five contracts came close to meeting recommended best practices. The standard contracts failed to include Federal privacy, IT security, or records management requirements and the individualized service contract failed to address many of the best practices discussed earlier. As a result, the NASA systems and data covered by these five contracts are at risk of compromise, which could adversely affect Agency operations or result in the loss of data. In addition, because none of the contracts specified how a provider's performance would be measured, reported, or enforced, NASA has no way to ensure adequate service levels are met, increasing the risk that Government funds could be misspent.

Table: Review of Contracts with NASA's Cloud-Computing Service Providers

Contract Has	Contract 1	Contract 2	Contract 3	Contract 4	Contract 5
Defined roles and responsibilities of parties	No	No	No	No	No
Guaranteed system availability level	Yes	Yes	No	No	Yes
Reporting of service level metrics	No	No	No	No	No
Penalties for not meeting service levels	No	Yes	No	No	No
E-discovery requirements	No	No	No	No	No
Data retention and destruction policies	No	No	No	No	No
Data privacy requirements	No	No	No	No	No
Defined incident handling practices	Yes	No	No	No	Yes
Third party certification of IT security program	No	Yes	No	No	Yes

Source: Office of Inspector General analysis of NASA cloud-computing contracts.

Moderate-Impact Cloud Service Failed to Meet Key IT Security Requirements

As part of this audit, we conducted a detailed security review of the moderate-impact systems for which NASA is using a public cloud environment, namely internal and external NASA web portals managed by eTouch and NSSC's Online Information Center hosted by RightNow, a division of Oracle Corporation. We focused on these systems because under NIST guidelines a security breach of a moderate-impact system could have serious adverse effects on the Agency. As part of our review, we assessed whether eTouch and RightNow met Federal and Agency certification and accreditation requirements. The certification and accreditation process is a risk management practice that enables managers to make informed decisions on the operation of IT systems or services. For example, by certifying and accrediting an IT system, management accepts responsibility for its security and is fully accountable for any adverse impacts to the Agency if a breach of security occurs. Moreover, according to Federal and Agency IT security requirements, systems must be certified and accredited before they are placed into operation and allowed to store and process data.

Although the service provider is responsible for meeting certification and accreditation requirements, NASA is responsible for ensuring that the service provider conducts the certification and accreditation process in accordance with Federal and Agency guidance.

We reviewed documentation provided by eTouch and RightNow, including systems security and contingency plans, authorization to operate the system, and the results of annual system control tests. We found that NASA's internal and external portal, which includes more than 100 websites, was operating without system security or contingency plans and with an operating authorization that expired in 2010. Even more troubling, a test of security controls on the IT services provided by the NASA Portal had never been undertaken to determine whether the system's controls were implemented correctly, operating as intended, and producing the desired result of securing the system and its data. These shortcomings occurred because NASA failed to adequately oversee eTouch to ensure that Federal and Agency IT security requirements were met. As noted below, NASA has replaced eTouch and implemented a contract with InfoZen, which addresses the IT security shortcomings, we identified. The other moderate-impact system, NSSC's Online Information Center operated by RightNow, met Federal and Agency IT security requirements.

NASA's Contract for Acquiring Cloud-Computing Services Meets Recommended Best Practices but NASA has Not Leveraged Its use Agency-wide

In December 2012, the Agency OCIO signed the NASA Web Enterprise Services Technology (WestPrime) contract with InfoZen. Under the WestPrime contract, InfoZen hosts more than 100 internal and external NASA websites and manages NASA's public

Internet portal. The WestPrime contract may be used to acquire web-based, cloud-computing services for systems having an IT security categorization rated as low or moderate impact. However, NASA has not leveraged this contract by requiring that all Agency organizations seeking to transfer systems and data to a public cloud use WestPrime. Nor has the Agency required that organizations use contracts with similar FedRAMP-compliant terms.

We found that the WestPrime contract includes the recommended best practices endorsed by the Federal CIO and Chief Acquisition Officer Councils. For example, we found that the contract specifies the respective roles and responsibilities of NASA, the cloud broker, and the cloud service providers. In addition, the contract contains standards for contractor performance, including how performance will be measured, reported, and enforced and addresses Federal privacy, discovery, data retention and destruction requirements, and incident detection and handling practices. Importantly, the contract also requires the broker and cloud providers to abide by FedRAMP security requirements. For example, the broker and all cloud provider IT security programs must be independently evaluated and certified in accordance with FedRAMP. The broker is also required to ensure any updates, testing, and support to the cloud environments follow FedRAMP; ensure protection and defense of cloud systems from recurring security threats and real-time vulnerabilities; and provide comprehensive auditing and appropriate patch management that adheres to FedRAMP. Finally, the contract requires semiannual reports to the Agency showing continuous monitoring of the broker and cloud providers' FedRAMP certifications and includes penalties for failing to meet these metrics.

NASA Satisfied Major Requirements of Cloud First Initiative

We found that NASA satisfied the requirement of OMB's Cloud First initiative to move several services to the cloud. Specifically, the Agency OCIO, Johnson, JPL, Marshall, and the NSSC each moved at least one IT service to a public cloud by December 2011, and the Agency OCIO, JPL, and Marshall each moved at least one additional IT service to a public cloud by June 2012. In addition, the Kennedy Space Center and Langley Research Center are evaluating public cloud services for office automation and scientific computing. Examples of the types of services NASA organizations have moved to the cloud include high-capacity computation and data storage to support climate modeling and content management for more than 100 internal and public-facing Agency websites, including NASA's public web portal www.nasa.gov.

Conclusion

At the time of our audit, five NASA organizations had implemented cloud services and two other Centers were exploring how to leverage cloud technologies to increase operational efficiencies. Moreover, NASA projects significant increases in cloud deployments in the next 5 years when up to 75 percent of new IT programs could begin

in the cloud and up to 40 percent of legacy systems could be moved to the cloud. As NASA expands its use of public cloud services, it is imperative that the Agency strengthen its governance and risk management practices to mitigate the chance that Agency operations may be disrupted, data lost, or public funds misused. Moreover, improved coordination is needed between the Agency OCIO and NASA Centers to ensure unapproved and unsecured cloud services are not implemented, cloud-computing contracts incorporate best practices, and all FedRAMP requirements are met.

Recommendations, Management's Response, and Evaluation of Management's Response

To strengthen NASA's IT governance practices with respect to cloud computing, mitigate business and IT security risks, and improve contractor oversight, we recommend that the Agency CIO:

Recommendation 1. Establish a cloud-computing program management office with authority to promulgate cloud-computing strategy and related standards and approve, coordinate, and oversee Agency-wide acquisition of cloud-computing services.

Management's Response. The Agency CIO concurred with our recommendation stating that in August 2011, his office established the Computing Services Service Office (CSSO) as the NASA entity responsible for all computing related services including data center consolidation and cloud computing. Moreover, the CSSO is also responsible for establishing an enterprise management approach for cloud computing and developing processes to ensure Agency-wide FedRAMP compliance. Further, by September 30, 2014, the Agency CIO will:

- revise and strengthen the CSSO's charter based on our audit findings and recommendations,
- formally communicate to all NASA organizations that the CSSO is the Agency's focal point for cloud computing and FedRAMP, and
- develop and publish guidance on use and acquisition of cloud-computing services at NASA.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 2. Require that NASA organizations use the WestPrime contract or a contract that helps ensure risks are mitigated and FedRAMP requirements are met when acquiring cloud-computing services.

Management's Response. The Agency CIO concurred with our recommendation and stated that by September 30, 2014, he would:

- require that all NASA organizations use the WestPrime contract for purchasing cloud-based web services,
- establish Agency-wide vehicles (contracts) for obtaining commercial cloud services with selected providers and require all NASA organizations use these vehicles when purchasing commercial cloud services, and
- publish policies and guidelines to be followed Agency-wide when acquiring commercial cloud services.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 3. Ensure any movement of moderate- or high-impact NASA systems to public clouds conforms with Federal and Agency IT security requirements.

Management's Response. The Agency CIO concurred with our recommendation and stated that by September 30, 2014, OCIO would establish policies and procedures requiring NASA organizations to register all purchases of cloud services with the CSSO to ensure that all IT security requirements are met.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

To ensure that NASA's existing cloud-computing services meet FedRAMP requirements, we recommend that the Agency CIO:

Recommendation 4. Direct all NASA CIOs to review FedRAMP and take necessary action to ensure their existing and planned cloud-computing services meet FedRAMP requirements.

Management's Response. The Agency CIO concurred with our recommendation and stated that by September 30, 2014, he would formalize policies and procedures for complying with FedRAMP and require that NASA organizations seeking to acquire cloud services work with CSSO's FedRAMP team to ensure that all FedRAMP requirements are met.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

To remedy IT security risks associated with the moderate-impact system (managed by eTouch) we identified as operating without system security or contingency plans, we recommend that the system owner:

Recommendation 5. Require the cloud service provider or broker to develop NIST-compliant security and contingency plans and conduct a test of the system's security controls.

Management's Response. The Agency CIO concurred with our recommendation and stated that NASA's web services contract with cloud-computing provider eTouch has been terminated and that all legacy eTouch infrastructure will be shut down by September 30, 2013. Further, he will ensure that the new system (managed by InfoZen) meets Federal and Agency IT security requirements.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 6. Ensure that the responsible Information Security Officer review IT security documentation and control tests and authorize the system for operation, as appropriate.

Management's Response. The Agency CIO concurred with our recommendation and again stated that NASA's web services contract with eTouch has been terminated and that all legacy eTouch infrastructure will be shut down by September 30, 2013. Further, the CIO will ensure that the new system meets Federal and Agency IT security requirements.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

APPENDIX A

Scope and Methodology

We performed this audit from June 2012 through June 2013 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.

In order to determine the adequacy of the Agency's governance model and risk management practices, we selected samples of cloud-computing services for detailed review. To determine the Agency's portfolio of cloud-computing services, we sent questionnaires to the Center, Headquarters, NSSC, and Mission Directorate CIOs. Based on the results of the surveys, we identified all projects currently hosting data with third-party cloud providers for our governance objective. For these projects, we interviewed NASA and contractor staff responsible for the projects and reviewed the contracts and service level agreements to determine whether they clearly defined the responsibilities of the parties; defined performance in clear terms; and stated how performance would be measured, reported, and enforced. We also assessed whether the contracts addressed Federal privacy, E-discovery (granting access to facilities for audit and investigative purposes), and data retention and destruction requirements. In addition, we selected all moderate or higher cloud services the Agency has contracted from a cloud service provider for detailed review. We interviewed NASA and contractor staff and obtained and reviewed the following documents to determine whether they met Federal and Agency IT security requirements, including incident detection and handling and third party certification of their IT security programs:

- System Security plan,
- most recent test of selected security controls,
- contingency plan,
- authorization to operate,
- cloud provider computer security incident handling policies and procedures, and
- independent assessment reports or certification of the cloud services the Agency receives from public cloud service providers.

Federal Laws, Regulations, Policies, and Guidance. We reviewed the following in the course of our audit work:

- Federal Information Security Management Act (FISMA) of 2002
- Office of Management and Budget Appendix III to OMB Circular No. A-130
- NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010
- NIST Special Publication 800-53A, Revision 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," June 2010
- NIST Special Publication 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012
- NPR 2810.1A, "Security of Information Technology," May 19, 2011
- IT Security Handbook 2810.02-02, "Security Assessment and Authorization: Information System Certification and Accreditation Process for FIPS 199 Moderate & High Systems," November 10, 2010
- IT Security Handbook 2810.02-04, "Security Assessment and Authorization: Continuous Monitoring - Annual Security Control Assessments," November 10, 2010
- IT Security Handbook 2810.02-05, "Security Assessment and Authorization: External Information Systems," November 8, 2010
- IT Security Handbook 2810.09-02, "Incident Response and Management: NASA Information Security Incident Management," August 24, 2011

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Review of Internal Controls

We reviewed internal controls related to the oversight of cloud-computing providers and security of Agency cloud-computing technologies. This included determining whether NASA has policies and procedures in place specific to cloud-computing technologies.

Prior Coverage

During the last 5 years, the Government Accountability Office, Department of Energy Office of Inspector General, and Social Security Administration Office of Inspector General have issued six reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at http://www.gao.gov, http://energy.gov/ig/office-inspector-general, and http://oig.ssa.gov/, respectively.

Government Accountability Office

"Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges" (GAO-13-462T, March 7, 2013)

"Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned" (GAO-12-756, July 2012)

"Information Security: Additional Guidance Needed to Address Cloud Computing Concerns" (GAO-12-130T, October 6, 2011)

"Information Security: Governmentwide Guidance Needed to Assist Agencies in Implementing *Cloud Computing*" (GAO-10-855T, July 1, 2010)

Department of Energy Office of Inspector General

"Department's Management of Cloud Computing Services" (OAS-RA-L-11-06, April 2011)

Social Security Administration Office of Inspector General

"Cloud Computing at the Social Security Administration" (A-14-12-11226, September 2012)

MANAGEMENT COMMENTS

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

JUL 24 2013

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Response to OIG Draft Report, "NASA's Progress Adopting Cloud Computing Technologies" (Assignment No. A-12-022-00).

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review and provide comments on the Office of Inspector General (OIG) draft report entitled, *"NASA's Progress Adopting Cloud Computing Technologies"* (Assignment No. A-12-022-00), dated June 12, 2013.

In the draft report the OIG makes six recommendations intended to strengthen the Agency's IT governance and risk management practices. Specifically, the OIG recommends the following:

Recommendation 1: NASA's Chief Information Officer (CIO) establish a cloud-computing program management office authorized to promulgate an Agency cloud-computing strategy; define related standards; and approve, coordinate, and oversee Agency-wide acquisition and deployment of cloud-computing services.

Management's Response: OCIO concurs with the recommendation. In August 2011, OCIO chartered the Computing Services Service Office (CSSO) in the Enterprise Service and Integration Division of OCIO to be responsible for all computing related services including data center consolidation and cloud computing. This service office is a peer to the other five Information Technology Infrastructure Integration Program (I3P) services offices responsible for Communications Services, End User Services, Web Services, HelpDesk Services and Enterprise Application Services. The CSSO is working on the enterprise management approach to cloud computing for NASA and developing the processes for Agency Federal Risk Authorization Management Program (FedRAMP) compliance. The charter of the CSSO will be revised and strengthened to reflect the recommendations in the OIG report entitled, *"NASA's Progress Adopting Cloud Computing Technologies"* (Assignment No. A-12-022-00).

Milestones:

- Revise CSSO charter to strengthen its effectiveness and address the recommendations in the OIG draft report entitled, *"NASA's Progress Adopting Cloud Computing Technologies*" (Assignment No. A-12-022-00) (Completion 9/30/2013)
- Agency CIO issue letter directing that the CSSO is the focal point for cloud computing at NASA and for FedRAMP. (Additional items in subsequent recommendations/actions will be added) (Completion 9/30/13)
- Develop guidance on use and acquisition of cloud computing at NASA, iteratively through FY 2014

Estimated completion date: September 30, 2014

Recommendation 2: Require that NASA organizations use the WestPrime contract or a contract that helps ensure risks are mitigated and FedRAMP requirements are met when acquiring cloud-computing services.

Management's Response: OCIO concurs with the recommendation.
Milestones:

- Include in Agency CIO letter the direction that all web services be obtained via WestPrime or similar contract (Completion 9/30/13)
- Include in Agency CIO letter advisory that OCIO is in the process of establishing an agency-wide vehicle for obtaining commercial cloud services from one or more commercial providers and once those vehicles are in place, all acquisition of cloud services must be through those vehicles which will be compliant with industry and federal best practices (Completion 9/30/13).
- Document these policies and guidelines in formal policy, iteratively throughout FY 2014.

Estimated completion date: September 30, 2014

Recommendation 3: Ensure any movement of moderate or high-impact NASA systems to public clouds conforms with Federal and Agency IT security requirements.

Management's Response: OCIO concurs with the recommendation.

Milestones:

- Establish policy and procedures that any cloud service purchased at NASA whether directly or via support contractor or by purchase card, etc. must be registered with OCIO's CSSO. (Completion 9/30/13)
- NASA CIO letter document this policy (Completion 9/30/13)
- Formalize this policy and a procedure in CSSO documentation, iteratively throughout FY 2014

Estimated completion date: September 30, 2014

Recommendation 4: Direct all Center and Mission Directorate CIOs to review FedRAMP and take necessary actions to ensure their existing and planned cloud-computing services meet FedRAMP requirements.

Management's Response: OCIO concurs with the recommendation. We have already begun to work with new cloud projects to advise them of our umbrella approach to FedRAMP compliance, explain the various roles and responsibilities and explain the FISMA and other integration points they must interface with to be fully compliant with IT security requirements.

Milestones:

- In NASA CIO letter, advise that anyone obtaining cloud services must work with OCIO's CSSO FedRAMP team to understand and comply with NASA's IT security approach to cloud (Completion 9/30/13).
- Formalize this policy and procedures in CSSO documentation, iteratively throughout FY14.

Estimated completion date: September 30, 2014

Recommendation 5: Require the cloud service provider or broker develop NIST-compliant security and contingency plans and conduct a test of the system's security controls.

Management's Response: OCIO concurs with the recommendation. The legacy eTouch infrastructure will be shut down when the eTouch contract ends. In anticipation of system shutdown, no further assessments or plans or testing will be performed.

Milestone: Shut down the legacy eTouch infrastructure.

Estimated completion date: September 30, 2013

Recommendation 6: Ensure that the responsible Information Security Officer review IT security documentation and control tests and authorize the system for operation, as appropriate.

Management's Response: OCIO concurs with the recommendation. As referenced in the OIG Audit Report, this recommendation is pertaining to the legacy eTouch infrastructure, which is being shut down in September 2013. In anticipation of system shutdown, no further assessments or plans or testing will be performed. OCIO will ensure that the new system meets security requirements based on this recommendation.

Milestone: Shut down the legacy eTouch infrastructure.

Estimated completion date: September 30, 2013

The recommendations are feasible; however, the implementation of the recommendations is contingent upon the availability of funds.

Again, thank you for the opportunity to review and comment on the subject draft report. If you have further questions or require additional information on the NASA response to the draft report, please contact Karen Petraska at 202-358-3722.

Larry N. Sweet
Chief Information Officer

cc:
Office of the Chief Information Officer/Ms. Burks
Office of the Chief Information Officer/J.C. Duh

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer

Non-NASA Organizations and Individuals

Office of Management and Budget
    Deputy Associate Director, Energy and Science Division
        Branch Chief, Science and Space Programs Branch
Government Accountability Office
    Director, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
    Subcommittee on Commerce, Justice, Science, and Related Agencies
Senate Committee on Commerce, Science, and Transportation
    Subcommittee on Science and Space
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
    Subcommittee on Commerce, Justice, Science, and Related Agencies
House Committee on Oversight and Government Reform
    Subcommittee on Government Operations
House Committee on Science, Space, and Technology
    Subcommittee on Oversight
    Subcommittee on Space

Major Contributors to the Report:

Wen Song, Director Information Technology Audit
Jefferson Gilkeson, Program Manager
Morgan Reynolds, Audit Team Lead

JULY 29, 2013

REPORT No. IG-13-021

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY13/ to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at Laurence.B.Hawkins@nasa.gov or call 202-358-1543.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD). You may also write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026, or use http://oig.nasa.gov/hotline.html#form. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.