NASA

National Aeronautics and Space Administration

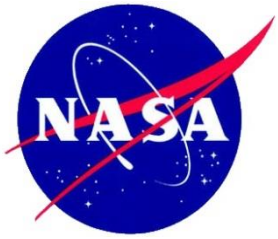
Office of Inspector General

Office of Audits

SECURITY OF NASA'S CLOUD COMPUTING SERVICES

February 7, 2017

Report No. IG-17-010



Office of Inspector General

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

To suggest ideas for or to request future audits contact the Assistant Inspector General for Audits at https://oig.nasa.gov/aboutAll.html.

NASA Office of Inspector General
Office of Audits

RESULTS IN BRIEF

Security of NASA's Cloud Computing Services

February 7, 2017 IG-17-010 (A-16-002-00)

WHY WE PERFORMED THIS AUDIT

NASA's information technology (IT) portfolio includes systems that control spacecraft, collect and process scientific data, provide security for critical infrastructure, and enable Agency personnel to collaborate with colleagues around the world. In fiscal year 2016, the Agency spent approximately $1.4 billion on IT investments in support of its mission. Among these investments was the acquisition of cloud computing services from commercial companies.

To accelerate the Federal Government's use of cloud computing, the Office of Management and Budget (OMB) in 2011 required agencies to adopt a "Cloud First" policy when contemplating IT purchases and to evaluate secure, reliable, and cost effective cloud computing alternatives when making new IT investments. To help Federal agencies meet these requirements, the General Services Administration collaborated with the National Institute of Standards and Technology and the Departments of Defense and Homeland Security to establish the Federal Risk and Authorization Management Program (FedRAMP). Since June 2014, Federal agencies have been required to ensure their cloud services are FedRAMP approved.

In July 2013, we reported that weaknesses in NASA's IT risk management and governance practices had impeded the Agency from fully realizing the benefits of cloud computing and potentially put NASA systems and data stored in the cloud at risk. The objective of this audit was to reassess NASA's cloud computing efforts and examine whether the Agency has effectively implemented plans, procedures, and controls to meet Federal and Agency IT security requirements for protecting the confidentiality, integrity, and availability of data stored in the cloud. To complete this work, we reviewed all applicable Federal, Agency, and Center regulations and guidance.

WHAT WE FOUND

While NASA has made improvements since our 2013 audit, continuing weaknesses in its governance and risk management processes have prevented the Agency from fully realizing the benefits of cloud computing and continue to leave Agency information stored in cloud environments at unnecessary risk. The Office of the Chief Information Officer (OCIO) made available to Agency staff three FedRAMP-compliant cloud computing services and approved 19 others for use. It has also moved just over 1 percent of eligible Agency data into approved cloud services. In addition, in an effort to capture the universe of services in use at the Agency, the OCIO created a cloud services registry.

However, NASA has not completed the necessary steps to ensure all approved services are registered with FedRAMP. Further, several of the services on the registry lacked authorizations to operate and were not covered by an IT system security plan. We also discovered an additional 20 cloud services in use at NASA not on the registry. Although 14 of these services had been approved and authorized by Center IT security officials, 6 lacked authorizations to operate or system security plans and had not been tested for appropriate security controls. We also identified numerous instances in which Agency personnel acquired cloud services using contracts that lacked provisions intended to address key business and IT security risks associated with cloud environments. As NASA continues to move more data to the cloud, it is imperative the Agency strengthen its risk management and governance practices to safeguard its information.

WHAT WE RECOMMENDED

To strengthen security controls over cloud computing, we made the following six recommendations to the NASA Chief Information Officer: (1) monitor adherence to the requirement that only approved cloud computing services be used and block access on NASA networks for unapproved services; (2) ensure acquisition of any cloud computing services are properly coordinated and accounted for on the Agency's cloud services registry and that all recommended contract provisions are incorporated into the acquisition; (3) ensure NASA's portfolio of approved cloud computing services is sufficient to meet Agency needs; (4) ensure all approved cloud services are registered with FedRAMP and are FedRAMP compliant; (5) ensure information on the use of and risks associated with cloud computing is incorporated into NASA IT security training; and (6) direct all NASA Centers, Mission Directorates, and Program and Project Offices to review current cloud computing services and take necessary steps to ensure existing services meet FedRAMP requirements.

In response to a draft of our report, the NASA Chief Information Officer concurred or partially concurred with our recommendations and described corrective actions the Agency will take to address them. We consider the proposed actions responsive to recommendations 1, 3, and 5 and will close these recommendations upon verification and completion of the proposed actions. We consider management's responses to recommendation 4 nonresponsive and to recommendations 2 and 6 only partially responsive. Accordingly, these recommendations will remain unresolved pending further discussion with the Agency.

For more information on the NASA Office of Inspector General and to view this and other reports visit https://oig.nasa.gov/.

TABLE OF CONTENTS

Acronyms

CIO	Chief Information Officer
CSPO	Computing Services Program Office
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act of 2002
GA4G	Google Apps for Government
GAO	Government Accountability Office
IT	Information Technology
ITS-HBK	Information Technology Security Handbook
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication

INTRODUCTION

NASA's information technology (IT) portfolio includes systems that control spacecraft, collect and process scientific data, provide security for critical infrastructure, and enable Agency personnel to collaborate with colleagues around the world. In fiscal year 2016, the Agency spent approximately $1.4 billion on IT investments in support of its mission. Among these investments was the acquisition of cloud computing services from commercial companies.

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 interaction.[1] In other words, in the cloud environment, IT resources are available to users as needed on a pay-as-you-go basis. While 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, it also poses risks, most prominently limited control over the management of critical or sensitive data stored in the cloud environment. Consequently, proper governance over the use of cloud computing services, to include effective management of contractor performance, is critical to ensure key business and IT security requirements are met and Agency data stored in the cloud is adequately protected.

NASA uses cloud computing to address a number of important functions, including large-scale computational services to support 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 infrastructure, cloud computing allows NASA scientists and engineers to use only the resources needed to complete a particular project or function.

In 2013, we reported that weaknesses in NASA's IT risk management and governance practices had impeded the Agency from fully realizing the benefits of cloud computing and potentially put NASA systems and data stored in the cloud at risk.[2] We noted certain contracts NASA had used to acquire cloud computing services failed to address or mitigate key business and IT security risks associated with use of the cloud. In addition, we found the Agency's Office of the Chief Information Officer (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. We made six recommendations to NASA, and the Agency has since taken action to address them.

[1] NIST Special Publication (SP) 800-145, "The NIST Definition of Cloud Computing," September 2011.

[2] NASA Office of Inspector General, "NASA's Progress In Adopting Cloud-Computing Technologies" (IG-13-021, July 29, 2013).

The objective of this audit was to reassess NASA's cloud computing efforts and examine whether the Agency has effectively implemented plans, procedures, and controls to meet Federal and Agency IT security requirements for protecting the confidentiality, integrity, and availability of its data stored in the cloud. We also reviewed internal controls as they relate to the overall audit objective. Details of the audit's scope and methodology are outlined in Appendix A.

Background

To accelerate the Federal Government's use of cloud computing, the Office of Management and Budget (OMB) in 2011 required agencies to adopt a "Cloud First" policy when contemplating IT purchases and to evaluate secure, reliable, and cost-effective cloud computing alternatives when making new IT investments.[3] The emphasis on cloud computing can be traced to the five essential characteristics shared by cloud computing environments:

1. *On-demand self-service*. A consumer can unilaterally and automatically provision computing resources such as processing, data storage, and network bandwidth.
2. *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.
3. *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 knowledge of or control over the location of the provided resources.
4. *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.
5. *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.

To help Federal agencies meet the requirements of Cloud First, the General Services Administration collaborated with NIST and the Departments of Defense and Homeland Security to establish the Federal Risk and Authorization Management Program (FedRAMP). There are three main players in FedRAMP: the agencies that acquire the services, the companies that provide the services (providers), and the independent organizations that perform initial and periodic assessments of provider systems to determine whether they meet FedRAMP requirements (assessors). Since June 2014, Federal agencies have been required to ensure the cloud services they use are FedRAMP approved. As of November 2016, 76 cloud computing services had been certified FedRAMP approved.

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

Risk Management for Cloud Computing

According to NIST, assessing and managing the risks of transferring to and maintaining systems and data in a public cloud is particularly challenging because the computing environment is under the control of the provider rather than the agency. Accordingly, effective risk mitigation requires development of system security plans that document and provide an overview of security requirements and describe the controls in place or planned to meet those requirements. Further, contracts must be developed that address business and security risks unique to cloud computing environments. Specifically, contracts with providers should contain clauses explaining how their performance will be measured, reported, and enforced and how Federal privacy, litigation discovery, and data retention and destruction requirements will be met. In addition, contracts should identify how providers will perform such important IT security activities as incident detection and require that providers' security programs be evaluated and certified periodically by an independent third party. Finally, attention to the roles and responsibilities of the Agency and the provider are required to drive contractor performance and ensure Agency systems and data are adequately secured.

FedRAMP Contract Clauses

As a best practice, the Federal Chief Information Officer (CIO) and Chief Acquisition Officer Councils recommend 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. In addition, FedRAMP recommends contracts with cloud service providers include 12 clauses that address security controls, such as those that protect against unauthorized disclosure of information and ensure appropriate record retention and accountability for digital signatures (see Appendix B for a summary of all 12 clauses).[4]

Federal IT Inventory Requirements

The Federal Information Security Management Act (FISMA) of 2002 requires Federal agencies to have an information systems inventory that identifies interfaces between all agency systems and networks, including those operated by or under the control of outside entities such as cloud providers. Further, all information systems in the inventory should be categorized using NIST's Federal Information Processing Standards Publication (FIPS PUB) 199, which provides a framework to help agencies categorize their information and information systems based on risk. FIPS PUB 199 categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems the organization needs to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Under FIPS PUB 199, information systems may have a low, moderate, or high impact security level. A security impact level is considered "low" when the loss of confidentiality, integrity, or availability could be expected to have a "limited" adverse effect on organizational operations, assets, or individuals. A security impact level is "moderate" when the loss could be expected to have a "serious" adverse effect and "high" when the loss could be expected to have a "severe or catastrophic" adverse effect.[5] FedRAMP has established recommended security controls for cloud computing services based on whether the associated system has a low, moderate, or high security impact level.

---

[4] FedRAMP, "Control Specific Contract Clauses," V2.0, June 6, 2014.

[5] NIST FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

FedRAMP Security Assessment Framework

FISMA requires Federal agencies to develop and manage system security plans that document and provide an overview of security requirements and describe the controls in place or planned for meeting those requirements.[6] The security plan also delineates responsibilities and expected behavior of all individuals who access the system. FedRAMP's security assessment framework guides the completion of system security plans in a manner compliant with FISMA and based on NIST security requirements.[7] Upon completion of the security plan, and at least every 3 years thereafter, a senior agency management official must authorize the system to operate.[8] In making such an authorization, the manager accepts the condition of the control environment and any associated risk. Management authorization should be based on an assessment of management, operational, and technical controls. (See Appendix C for the types of controls documented in a system security plan.)

Governance over Use of Commercial Cloud Computing at NASA

During the last 6 years, the NASA Office of Inspector General (OIG) has issued over 20 audit reports containing more than 80 recommendations designed to improve NASA's IT security efforts, including a 2013 audit which found that NASA has struggled to implement an effective IT governance approach that appropriately aligns authority and responsibility commensurate with the Agency's overall mission.[9] In addition, in our 2016 FISMA review we noted that even as NASA works to address more effective IT risk management and governance practices, IT security remains a significant challenge for the Agency.[10]

As noted in our July 2013 report on cloud computing, effectively managing the delivery of commercial cloud computing services requires agencies to develop contracts that address business and security risks as well as provide 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 of commercial cloud providers and the ease with which their services can be acquired – including some available at no or a very low cost – a lack of organizational control over the acquisition of cloud services can create problems. For example, if cloud computing services are acquired without proper evaluation, approval, and oversight, vulnerable systems and sensitive information may be placed in the cloud, legal and privacy requirements may not be met, and cost efficiencies lost.

In August 2011, the NASA CIO established the Computing Services Service Office and charged it with responsibility for all computing-related services, including cloud computing and data center consolidation. In 2013, the NASA CIO directed Center CIOs to work with the Computing Services Service Office to establish a complete inventory of existing cloud computing services at NASA and to maintain an accurate and up-to-date portfolio of such services going forward. A comprehensive inventory of all

---

[6] NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010.

[7] NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006.

[8] Authorization of a system to process information at NASA often takes the form of an IT System Authorization to Operate. The Federal Government is in the process of transitioning to ongoing authorizations for information systems in accordance with NIST SP 800-37.

[9] NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

[10] NASA OIG, "Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation" (IG-17-002, November 7, 2016).

cloud services is a critical step on the path to FedRAMP compliance. According to OMB, agency inventories should accurately reflect their current information system, include all components within the authorization boundary of their system, and be of sufficient granularity to enable adequate tracking and reporting.[11]

New Cloud Management Office

In March 2016, the Computing Services Service Office was renamed the Computing Services Program Office (CSPO) and directed to provide oversight of NASA's data center and cloud computing portfolios and to serve as the focal point for management and business activities of all OCIO computing services and related initiatives. CSPO develops cloud computing strategies and related standards to coordinate and oversee acquisition of cloud computing services Agency-wide and serves as the official NASA interface with FedRAMP and commercial cloud providers. According to Agency officials, CSPO will enhance the integration of Center IT personnel into the process of approving, acquiring, and delivering cloud services.

To facilitate cloud adoption at NASA, reduce costs, and increase compliance with Federal requirements, in March 2016, CSPO established an enterprise-managed cloud computing framework. Center CIOs were each asked to designate a point of contact to coordinate between the Center's cloud customers and the CSPO. NASA intends that all "raw" cloud computing – cloud services that provide primarily computing power and storage capacity as opposed to integration or development services – be acquired through Agency-provided acquisition vehicles to give NASA the best volume pricing and greatest security while limiting data sprawl.[12] According to Agency officials, NASA's goal is to reach a state in which all cloud computing services in use at the Agency are "managed" services that properly integrate with the Agency's infrastructure and are compliant with Agency IT governance and security policies. In an effort to help meet the Agency's requirements, NASA established the Cloud Computing Community of Interest to help inform personnel of a broad range of available cloud computing opportunities. The Community includes NASA employees and contractors and typically hosts guest speakers who present information and afford participants the opportunity to discuss issues during a question and answer session.

As part of this audit, we requested from the OCIO an inventory of cloud computing services in use at NASA. The OCIO provided us with a copy of a registry that lists 30 cloud services, 22 of which had been approved by the OCIO for use at the Agency. The OCIO learned about the other 8 services while testing a Cloud Access Security Broker tool at two Centers on a trial basis for potential use Agency-wide. At the time of our field work, these 8 services were being used by Agency personnel but we were unable to determine whether they had been approved for use Agency-wide or at the Center level.

[11] OMB M-14-04, "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," November 18, 2013.

[12] Data sprawl describes the phenomena that once data leaves a system it is out of the immediate control of the owner.

NASA Needs to Improve Its Cloud Computing Risk Management and Governance Processes

While NASA has made improvements since our 2013 audit, continuing weaknesses in its risk management and governance processes have prevented the Agency from fully realizing the benefits of cloud computing and continue to leave Agency information stored in cloud environments at unnecessary risk. The OCIO has made available to Agency staff three FedRAMP-compliant cloud computing services and approved 19 others for use. It has also moved just over 1 percent of eligible data into approved services.[13] Moreover, in an effort to capture the universe of services in use at the Agency, the OCIO created a cloud services registry. However, NASA has not completed the necessary steps to ensure all approved services are registered with FedRAMP. Further, several of the services on the registry lacked authorizations to operate and were not covered by an IT system security plan. We also discovered an additional 20 cloud services in use at NASA not on the registry. Although 14 of these services had been approved and authorized by Center officials, 6 lacked authorizations to operate or system security plans and had not been tested for appropriate security controls. In addition, we identified numerous instances in which Agency personnel acquired cloud services using contracts that lacked provisions intended to address key business and IT security risks associated with cloud environments. As NASA moves more data to the cloud, it is imperative the Agency strengthen its risk management and governance practices to safeguard its information.

NASA's Management of Cloud Computing Services

As noted earlier, development and maintenance of an accurate inventory of the cloud services in use at an agency is necessary to maintain security and availability of data stored in the cloud. Personnel responsible for protecting NASA networks, systems, and data must know what services are being used to ensure they are covered by adequate security plans and authorized for operation on Agency networks. Furthermore, NASA's ability to protect data in the cloud is impaired when cloud services are acquired without a contract or with contracts that do not incorporate provisions to ensure proper security in the cloud environment.

[13] In August 2016, NASA estimated that 35 petabytes of its approximate 195 petabytes of data is appropriate for storage in the cloud with the bulk of its data deemed too sensitive for storage in the cloud environment. One petabyte is equal to 1,000,000,000,000,000 bytes or 1,000 terabytes.

Management of Approved Cloud Computing Services

NASA's cloud services registry includes 30 cloud services, 22 of which have been authorized for use by the NASA OCIO. However, only 3 of the 22 services are FedRAMP-approved, while 2 more are awaiting approval.[14] Further, we found that NASA has not yet taken the steps necessary to register the remaining 17 OCIO-approved services with FedRAMP. We also noted that in 2016 NASA reported to OMB that as of February 2015 the Agency had met the requirement to use FedRAMP-approved providers for cloud services. While NASA uses a limited number of FedRAMP-approved cloud services, we are concerned that the manner in which the information was reported makes it appear as though NASA is in full compliance with OMB's requirement that agencies use only FedRAMP-approved cloud services.

The use of FedRAMP-approved cloud services is important to ensure the integrity and security of Agency data that is transferred, processed, or stored in cloud environments. As discussed previously, FedRAMP services have been examined and tested by assessors to ensure they include appropriate information security controls and otherwise comply with Federal requirements.

Unapproved Cloud Computing Services

One major challenge facing Federal agencies in today's interconnected world is the identification of "shadow IT" – IT on an agency's network that the CIO or Chief Information Security Officer did not purchase or authorize for use and is not aware is being used by agency personnel. Using a government purchase card and web browser, employees can purchase low-cost subscription licenses to cloud computing services and easily obtain applications that allow them to transmit, process, and store large amounts of data without the CIO's or Chief Information Security Officer's involvement or awareness. Indeed, in some cases, cloud storage services are free. The use of unapproved cloud storage services may expose NASA data, as well as Agency networks used to connect to the services, to significant security risks, including loss, theft, or destruction of data or breach of Agency networks.

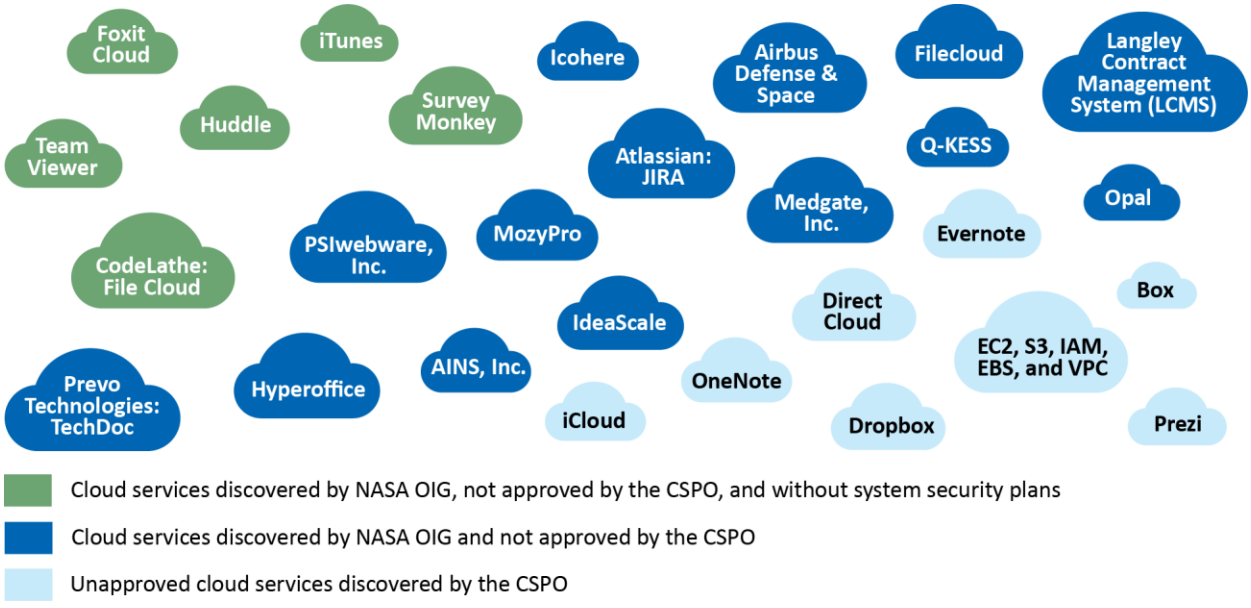
During the course of our audit, we learned of numerous unapproved cloud services in use at NASA. The OCIO itself identified and placed on the cloud services registry 8 services it had not approved. In addition, we identified 20 more services in use at NASA the OCIO was not aware of and had not approved.

As part of our audit fieldwork, we visited NASA Headquarters, Glenn Research Center, and Johnson Space Center and spoke with officials to determine what cloud services were in use at the Agency. Early in the audit, we identified a service in use at Glenn Research Center that did not appear on the cloud services registry. As a result, we sent 60 surveys to the CIOs at the other NASA Centers and IT representatives and managers from 50 Agency program and project offices about their use of cloud services; we received 22 responses (37 percent). Despite this moderate response rate, respondents identified 18 cloud services in use at their Centers that were not on the registry. We independently identified 2 additional services in use at the Agency but not included on the registry. Although 14 of these services had been approved and authorized to operate by Center officials, 6 lacked system security plans or authorizations to operate from any NASA official.

[14] The three cloud services registered with FedRAMP are Amazon Web Services, Oracle Service Cloud, and ServiceNow. Two others – iSight and PTC Cloud Services – were awaiting FedRAMP approval as of September 27, 2016.

The utilization of cloud services without NASA approval or awareness places Agency data stored there at unnecessary risk. For example, one service we discovered – TeamViewer – provides the capability for "automatic discovery" of nearby contacts and devices to make collaboration and interaction easier, as well as "file transfer" that allows users to share files of any size using convenient methods such as file manager, contextual menus, drag and drop, and a file box that can link to cloud storage providers. This capability could allow sensitive data to be accessed by unauthorized individuals. Similarly, Huddle, another unapproved service that facilitates collaboration among team members, allows files to be shared easily across devices, locations, and teams outside of NASA's firewall, and therefore could result in the same type of unauthorized access. Figure 1 depicts the cloud services in use at NASA that had not been approved by the OCIO. See Appendix D for a more detailed description of these services.

Figure 1: Unapproved Cloud Computing Services in Use at NASA



Source: NASA OIG analysis and Agency survey results.

The OCIO has issued policy memorandums and related guidance requiring personnel to utilize only cloud computing services approved by the Agency and has made the cloud services registry of approved cloud services available via an internal NASA website. However, there are no controls in place preventing Agency personnel from accessing and storing NASA data in unapproved cloud services. Moreover, at the time of our audit NASA was not using Cloud Access Security Broker tools that could help identify all cloud computing services in use across the Agency. In September 2016, NASA approved the purchase of a Cloud Access Security Broker tool, but it is unclear whether the Agency will implement the full functionality of the tool, which includes the ability to restrict access to unauthorized cloud computing services.

We spoke to the CIO about the use of unapproved cloud services by Agency personnel. She told us she is focused on establishing enterprise cloud computing solutions that will provide personnel with the services they need and believes users will naturally adjust to using approved services once the cloud culture at NASA is more mature. Accordingly, she indicated she is not overly concerned about smaller scale uses of unapproved services.

Testing of Cloud Services

We selected 12 cloud computing services for substantive audit testing, 7 of which had been approved by the OCIO. We found that 10 of the services were not compliant with Federal IT security requirements. Specifically, 3 of the services were storing data from systems that had not undergone a FIPS PUB 199 assessment to determine their security impact level, lacked a system security plan, and had not been authorized to operate by either the CIO or any other NASA authorizing official. Seven others were being used to transmit, store, or process moderate impact data, but the associated security plans were missing the 66 FedRAMP recommended security controls for moderate systems in their system security plans, including controls that address the confidentiality and integrity of information at rest and ensure the security of connections to external networks or information systems (a description of the recommended controls can be found in Appendix C).

According to OCIO representatives, NASA is currently deploying a Continuous Diagnostics and Mitigation project designed to generate, track, and monitor system security plans more effectively.[15] They expect to complete implementation of the new system by January 2017. According to OCIO representatives, in light of the ongoing deployment, they decided not to expend the time, money, and resources to incorporate the missing FedRAMP recommended security controls into the existing system that generates, stores, and maintains system security plan documentation.[16] While we appreciate the reason for this decision, it may take some time to update system security plans in the new system and we did not identify alternative controls that would mitigate the absence of the security controls in the interim. Further, failure to include these controls in IT security plans impairs NASA's ability to obtain FedRAMP approval of the associated cloud computing services.

Contracts and Agreements Lack Required Provisions

Of the 12 contracts and agreements reviewed, we determined that 9 cloud services in use at NASA were procured without appropriate security provisions regarding classified information and 5 were missing required protections for how information is stored in the cloud. Specifically, we found that two clauses addressing IT security were not included in 5 of the NASA cloud computing contracts reviewed.[17] Likewise, 6 did not include contract provisions requiring the contractor to afford the Agency access to the contractors and subcontractors' facilities, installations, operations, documentation, databases, and personnel associated with the performance of the contract. We also found 3 of the services were free and governed only by standard terms of use agreements that lack many FedRAMP and NASA requirements. In summary, all 12 contracts and agreements we examined were missing one or more critical provisions aimed at ensuring appropriate security over and access to NASA data stored in the cloud.

---

[15] The Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) project was designed to assist Federal departments and agencies with properly securing their systems and data. Through CDM, DHS provides departments and agencies with commercial off-the-shelf IT security tools that enable system and network administrators to identify cybersecurity risks related to their networks, including current vulnerabilities and configuration settings. Because CDM affects all Federal departments and agencies, all NASA Centers and missions are within the projects scope. In September 2015, DHS awarded a task order to Booz Allen Hamilton to implement CDM services at NASA, and Agency officials are working with the contractor to integrate the necessary information security tools for deployment.

[16] The CSPO also completed a risk assessment that compared FedRAMP recommended controls to the use of NIST controls and determined the residual risk of not including the entire suite of FedRAMP controls was minimal when the cloud services in use were FedRAMP approved. This risk assessment was approved by the OCIO.

[17] NASA Federal Acquisition Regulation Supplement 1852.204-75, "Security Classification Requirements," September 1989, which addresses performance of work under contracts, and 1852.204-76, "Security Requirements for Unclassified Information Technology Resources," January 2011, which requires contractors to protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources.

We also found that 10 of the service agreements did not include any of the recommended FedRAMP contract clauses. According to one Center procurement official, the clauses were not added because the requesting NASA offices did not advise them of the need for the clauses.[18] Further, the procurement official noted that in many cases cloud computing services are relatively low cost and can be purchased using a government purchase card, in which case there is no contract vehicle in which to incorporate the recommended FedRAMP clauses. Table 1 summarizes the security posture of the 12 cloud computing services we examined.

Table 1: Security Posture of 12 Cloud Computing Services Examined

Cloud Computing Service	FIPS PUB 199 Categorization Level	System Security Plan Contains FedRAMP Recommended Controls?	Cloud Computing Service Authorized for Use?
CSPO Approved and Authorized Cloud Services Tested			
Amazon (EC2, S3, IAM, EBS, VPC)	Moderate	No[a]	Yes
Google Apps for Work	Moderate	No[a]	Yes
Carpatha Airwatch	Low	Yes	Yes
ServiceNow Data Center Portfolio Management at Kennedy Space Center	Moderate	No[a]	Yes
ServiceNow (Project Portfolio Management, Asset Management)	Moderate	No[a]	Yes
Fiberlink MaaS360	Moderate	No[a]	Yes
WESTPrime – AWS	Moderate	No[a]	Yes
Audit Team Discovered Cloud Services Tested			
ServiceNow at Glenn Research Center	Moderate	No[a]	Yes
CSPO "Discovered" Cloud Services Tested			
Amazon (EC2, S3, IAM, EBS, VPC)	Low	Yes	Yes
iCloud	No FIPS PUB 199 assessment performed	Not covered by a system security plan	No
Box	No FIPS PUB 199 assessment performed	Not covered by a system security plan	No
Dropbox	No FIPS PUB 199 assessment performed	Not covered by a system security plan	No

Source: Information from NASA IT system security plans

[a] For information systems categorized "moderate," FedRAMP recommends an additional 66 controls.

Impact of Using Unapproved Cloud Services

Using cloud computing services that have not been authorized to operate by a NASA official and are not FedRAMP approved presents a material threat to the confidentiality, integrity, and availability of Agency data transmitted, processed, or stored there. Because the information security controls for such

[18] This issue of poorly constructed cloud contracts is a concern across the Federal government. In October 2016, the Federal CIO requested CIOs across the government survey their primary cloud contracts and identify clauses or other terms that address the protection of government information.

services have not been reviewed or tested by Agency information security personnel, the Agency has no assurance that Federal and Agency information security and privacy requirements have been properly incorporated into the agreement to address requirements. These requirements include, for example, the Government having unlimited data rights that establish ownership of the Agency's data in the cloud, contractual requirements identifying where "data-at-rest" (primary and replicated storage) shall be maintained, and sanitization of the data when no longer stored in the cloud.[19] Consequently, NASA has little to no control over the data stored in unauthorized cloud environments.

In July 2012, an external hack on Dropbox – one of the unapproved services used by NASA employees – exposed the email addresses and passwords of 68 million users. In 2016, when it appeared that someone was making the stolen information available for sale, Dropbox issued a notification to its customers and forced users that had not already done so to change their passwords. In response to this notification, NASA issued the following security alert to Agency personnel:

> The NASA Office of the Chief Information Officer is aware that a number of NASA personnel use Dropbox to store and transmit agency documents. The agency is taking proactive steps to limit the threat posed by this compromise. These risks include:
>
> - Loss of Sensitive Data: Compromise of the Confidentiality or integrity of sensitive NASA data, which may be stored in Dropbox. This includes storing Personally Identifiable Information (PII), Sensitive But Unclassified (SBU), and International Traffic in Arms Regulations (ITAR) information on non-NASA systems.
> - NASA Accounts: Compromise of NASA accounts caused by users who reuse their NASA password for Dropbox
> - Social Engineering: Use of compromised Dropbox accounts to target other NASA users.
>
> We need you to take immediate action to do **three things** if you have a Dropbox account that you have used to store NASA information**:**
>
> 1. Change your Dropbox password.
> 2. If you have stored sensitive NASA data in Dropbox -- including PII, SBU, and information covered by ITAR or Export Administration Regulations -- please contact the Security Operations Center (SOC) to ensure appropriate remediation actions are taken.
> 3. NASA users are REQUIRED to report if they have any sensitive NASA data in their Dropbox account (SBU, PII, ITAR, export sensitive, contractual data, proprietary data, network configuration or diagrams, etc., whether the document is properly marked as sensitive or not). Again, if you have sensitive NASA data in your Dropbox account, contact the NASA Security Operations Center.

As the Dropbox example illustrates, failure to follow the requirement to only use approved services to transmit, process, and store NASA data puts Agency data at risk of loss, theft, or compromise. Since issuing its security alert, NASA has confirmed that sensitive Agency data, including personally identifiable information and International Traffic in Arms Regulations data, was stored on the Dropbox cloud service and Agency officials are working with users to remove the data from the service.[20]

[19] "Data-at-rest" refers to the state of information when it is located on storage devices as specific components of information systems.

[20] International Traffic in Arms Regulations govern the export and temporary import of defense-related articles and services governed by 22 U.S.C. 2778 of the Arms Export Control Act and Executive Order 13637.

The threats to NASA data residing in the cloud are not limited to unapproved or unauthorized services. In December 2011, the OCIO's Technology and Innovation Division initiated a pilot program using Google Apps for Government (GA4G), a cloud-based solution that provides email and collaboration applications. The pilot program stipulated that only nonsensitive NASA data be placed in the cloud and enabled users to connect to GA4G using their existing Personal Identification Verification smartcards. A contractor on NASA's Web Services (WESTPrime) contract – one of five Agency-wide service contracts under NASA's IT Infrastructure Integration Program – subsequently conducted a security audit of the data stored in the GA4G cloud and found multiple sensitive documents (including International Traffic in Arms Regulations and Sensitive But Unclassified data). In addition, the pilot program was not covered by a system security plan and the Agency did not retain a network activity trail or other controls to monitor activity in the GA4G cloud.

Similarly, in 2015, the NASA Security Operations Center issued an alert related to a NASA account used to administer two internal NASA.gov websites hosted by Google that may have been compromised. We were unable to determine if the websites were actually compromised because neither Google nor NASA had retained a network connection log. Had the Agency taken the necessary steps to ensure all Federal IT security requirements were properly incorporated into Agency system security plans, it is possible that network logs would have been properly maintained, enabling a more detailed assessment of incident.

Finally, in October 2016, a NASA employee reported a vulnerability with a cloud service that had not been approved by the OCIO. Specifically, the employee identified a large amount of sensitive information stored in the cloud that was accessible to all users. The Agency ultimately determined that a misconfiguration in a program used to access the cloud-stored information had enabled Agency-wide viewing of the sensitive information. We spoke with the Chief Information Security Officer about this incident, who told us the service lacked a system security plan and was not FedRAMP approved. She also noted that given the service was procured outside the purview of the OCIO, the Agency did not use a single, Agency-wide procurement vehicle and instead, various Centers purchased their own licenses for the service. As a result, key controls and contractual provisions governing the security of information residing in the cloud service were not incorporated into the procurement contracts used to acquire this service. This unfortunate incident further showcases the importance of having controls in place to mitigate data vulnerability and enable the Agency access to and control over data stored in the cloud environment.

CONCLUSION

The cloud computing marketplace has grown exponentially over the past 5 years, mirroring the increasing complexity of cloud services and the threats and risks associated with storing Government data in the cloud. NASA has made improvements in its implementation of cloud computing since our 2013 audit, but continued weaknesses in the Agency's risk management and governance practices impeded its progress toward fully realizing the benefits of cloud computing. Moreover, these weaknesses placed Agency information stored in the cloud environment at risk. Specifically, since 2013 NASA has established three FedRAMP-approved cloud computing services for Agency use and has moved approximately 1.2 percent of its data into these environments. However, much of the Agency's cloud computing activity occurs outside of these FedRAMP-approved services. With NASA's increasing use of the cloud, it is imperative the Agency strengthen its risk management and governance practices to safeguard its data.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To strengthen security controls over cloud computing, we made the following six recommendations to the NASA Chief Information Officer:

1. Monitor adherence to the requirement that only approved cloud computing services on NASA's cloud services registry be used to transmit, process, and store NASA data and block access on NASA networks to unapproved services that do not have an authorization to operate and established IT system security plans.
2. Ensure NASA personnel at Agency Centers, Mission Directorates, and Program and Project Offices coordinate acquisition of any cloud computing service through CSPO to ensure cloud services are properly accounted for on the Agency's cloud services registry and that all recommended FedRAMP contract provisions are incorporated into the acquisition.
3. Ensure NASA's portfolio of approved cloud computing services is sufficient to meet Agency needs.
4. Ensure all approved cloud services are registered with FedRAMP and are FedRAMP compliant.
5. Incorporate information on the use of and risks associated with cloud computing into required IT security training for all NASA employees.
6. Direct all NASA Centers, Mission Directorates, and Program and Project Offices to review their current cloud computing services and take steps necessary to ensure that existing services meet FedRAMP requirements.

We provided a draft of this report to NASA management who concurred or partially concurred with our six recommendations and described corrective actions the Agency will take to address them. We consider the proposed actions for recommendations 1, 3, and 5 to be responsive and will close the recommendations upon verification and completion of the proposed actions.

While the Agency concurred with recommendation 2, management's response only partially addresses the recommendation. Specifically, the proposed corrective action speaks to the development of standard contract clauses for use in cloud service acquisitions but fails to address the need for personnel at NASA Centers, Mission Directorates, and Program and Project Offices to coordinate acquisition of any cloud computing service through the CSPO to ensure cloud services are properly accounted for on the Agency's cloud services registry. As such, this recommendation will remain unresolved pending further discussion with the Agency.

Management partially concurred with recommendation 4 and described proposed corrective action. However, we do not believe the proposed action meets the intent of our recommendation. Specifically, management noted that "'officially' FedRAMP-approved products represent only 0.5 percent of available cloud products" and that less than 100 FedRAMP authorizations have been granted since the FedRAMP mandate went into effect in June 2014. According to management, the relatively low number of FedRAMP-approved products inhibits Federal agencies from fully adopting the "Cloud First" approach

to replacing information technology resources with cloud solutions. As such, management indicated NASA will use FedRAMP-approved cloud services whenever available but may make a risk-based decision to use non-FedRAMP-approved services. We are not aware of any instances in which NASA requested but was denied FedRAMP approval for a particular cloud service or any instances in which FedRAMP did not respond to an Agency approval request in a timely fashion. Accordingly, we do not agree that NASA cannot meet the Agency's needs for cloud services using only FedRAMP-approved services. As such, this recommendation remains unresolved pending further discussion with the Agency.

Finally, although management concurred with recommendation 6, we consider the proposed corrective action only partially responsive because it did not include a plan for ensuring existing cloud services meet FedRAMP-specific IT security requirements. Accordingly, the recommendation remains unresolved pending further discussion with the Agency.

Management's full response to our report is reproduced in Appendix E. Technical comments provided by management have also been incorporated, as appropriate.

Major contributors to this report include, Laura B. Nicolosi, Mission Support Director; Joseph A. Shook, Project Manager; Gina Davenport-Bartholomew; Teran W. Taggart; Sarah McGrath; and Earl E. Baker.

If you have questions about this report or wish to comment on the quality or usefulness of this report, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202 358 1543 or laurence.b.hawkins@nasa.gov.

Paul K. Martin
Inspector General

APPENDIX A: SCOPE AND METHODOLOGY

We preformed this audit from November 2015 through December 2016 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.

Our objective was to determine the effectiveness of NASA's information security controls relating to cloud computing services. Specifically, we determined whether NASA had established and implemented Agency-wide plans, procedures, and controls to meet Federal and Agency information technology security requirements to protect the confidentiality, integrity, and availability of NASA data maintained by cloud service providers. We also reviewed internal controls as they related to the overall objective. We performed our fieldwork at NASA Headquarters, Glenn Research Center, and Johnson Space Center.

Federal Laws, Regulations, Policies, and Guidance

We identified and reviewed all applicable Federal, Agency, and Center level regulations and guidance, including public laws; OMB, NIST, and FedRAMP guidance; FIPS publications; and NASA Policy Directives (NPD), NASA Procedural Requirements (NPR), and IT Security Handbooks.

Federal Laws, Regulations, Policies, and Requirements

- Pub. L. No. 113-283, "Federal Information Security Modernization of 2014," December 18, 2014
- Pub. L. No. 107-347, "E-Government Act of 2002," December 17, 2002
- 14 Code of Federal Regulations Part 1852.204-75, "Security Classification Requirements," September 1989
- 14 Code of Federal Regulations Part 1852.204-76, "Security Requirements for Unclassified Information Technology Resources," January 2011

Office Management and Budget

- OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," December 29, 2015
- OMB Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011

Federal Information Processing Standards Publications

- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

National Institute of Standards and Technology

- NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," June 2015
- NIST SP 800-146, "Cloud Computing Synopsis and Recommendations," May 2012
- NIST SP 800-145, "The NIST Definition of Cloud Computing," September 2011
- NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing," December 2011
- NIST SP 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," December 2014
- NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013
- NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," August 2002
- NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010
- NIST SP 800-30 rev 1, "Guide for Conducting Risk Assessments," September 2012
- NIST SP 800-18 rev 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006
- NIST SP500-292, "NIST Cloud Computing Reference Architecture," September 2011

Federal Risk and Authorization Management Program

- FedRAMP Security Assessment Framework, "Security Assessment Framework v2.1," December 4, 2015
- FedRAMP Agency Guide for FedRAMP Authorizations, "Agency Guide for FedRAMP Authorizations v1.0 FINAL," August 5, 2015
- FedRAMP Package Validation Process, "Package Validation Process FINAL," June 6, 2014
- FedRAMP Guide to Understanding FedRAMP, “Guide to Understanding FedRAMP, V2.0," June 6, 2014
- FedRAMP Continuous Monitoring Strategy & Guide, "Continuous Monitoring Strategy & Guide v2.0," June 6, 2014
- FedRAMP Control Specific Contract Clauses, "Control Specific Contract Clauses v2.0," June 6, 2014
- FedRAMP Standard Contract Language, "FedRAMP Standard Contractual Clauses 062712," June 27, 2012

NASA Policy Directives and Procedural Requirements

- NPD 2810.1E, “NASA Information Security Policy," June 14, 2015

- NPD 2540.1H, "Personal Use of Government Office Equipment Including Information Technology," February 24, 2016
- NPD 1382.17H, “NASA Privacy Policy," June 24, 2009
- NPR 2810.1A, “Security of Information Technology," May 16, 2006
- NPR 2800.1B, “Managing Information Technology," March 20, 2009
- NPR 1441.1E, “NASA Records Management Program Requirements, Chapter 5. Requirements for Management of Records in E-mail, Cloud, and Social Media,” January 29, 2015
- NPR 1382.1A, “NASA Privacy Procedural Requirements," July 10, 2013

NASA Information Technology Security Handbook (ITS-HBK)

- ITS Handbook (ITS-HBK)2810.18-01, "System and Communications Protection," May 6, 2011
- ITS-HBK 2810.17-01, "Identification and Authentication," January 17, 2011
- ITS-HBK 2810.16-01, "Audit and Accountability," May 6, 2011
- ITS-HBK 2810.14-01, "System and Information Integrity," December 1, 2014
- ITS-HBK 2810.06-01, "Security Awareness and Training," May 6, 2011
- ITS-HBK 2810.05-01, "Systems and Service Acquisition," November 21, 2011
- ITS-HBK 2810.04-03, " Risk Assessment: Web Application Security Program," April 30, 2013
- ITS-HBK 2810.04-02A, " Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement," April 30, 2013
- ITS-HBK 2810.04-01A, " Risk Assessment: Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching, & Organizationally Defined Values," October 12, 2012
- ITS-HBK 2810.02-05A, "Security Assessment and Authorization: External Information Systems", February 4, 2016
- ITS-HBK 2810.02-05, "Security Assessment and Authorization: External Information Systems," October 24, 2012

Use of Computer-Processed Data

We used computer-processed data to perform this audit, and that data was used to materially support findings, conclusions, and recommendations. In order to assess the quality and reliability of the data, we verified the information through independent calculations and corroboration with Program documents and the input of various Program officials. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

Review of Internal Controls

We reviewed internal controls as they relate to NASA’s use of cloud computing to transmit, process, and store Agency data and information. We discussed the control weaknesses identified in the body of this report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the last 5 years, the NASA OIG and the Government Accountability Office (GAO) have issued 21 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at http://oig.nasa.gov/audits/reports/FY17 and http://www.gao.gov, respectively.

NASA Office of Inspector General

Review of NASA's Information Security Program (IG-16-016, April 14, 2016)

Federal Information Security Management Act: Fiscal Year 2015 Evaluation (IG-16-002, October 19, 2015)

Federal Information Security Management Act: Fiscal Year 2014 Evaluation (IG-15-004, November 13, 2014)

NASA's Progress in Adopting Cloud-Computing Technologies (IG-13-021, July 29, 2013)

NASA's Information Technology Governance (IG-13-015, June 5, 2013)

Federal Information Security Management Act: Fiscal Year 2013 Evaluation (IG-14-004, November 20, 2013)

NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools (IG-13-006, March 18, 2013)

Final Memorandum, Federal Information Security Management Act: Fiscal Year 2012 Evaluation (IG-13-001, October 10, 2012)

NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems (IG-12-006, December 5, 2011)

Final Memorandum, Federal Information Security Management Act: Fiscal Year 2011 Evaluation (IG-12-002, October 17, 2011)

Government Accountability Office

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs (GAO-15-714, September 29, 2015)

Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems (GAO-15-573T, April 22, 2015)

Information Technology: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked (GAO-15-296, April 16, 2015)

Cloud Computing: Additional Opportunities and Savings Need to Be Pursued (GAO-14-753, September 25, 2014)

Information Technology: OMB and Agencies Need to Focus Continued Attention on Eliminating Duplicative Investments (GAO-13-685T, June 11, 2013)

2013 Annual Report: Actions Needed to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits (GAO-13-279SP, April 9, 2013)

Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned (GAO-12-756, July 11, 2012)

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

Information Technology: OMB Needs to Improve Its Guidance on IT Investments (GAO-11-826, September 29, 2011)

Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management (GAO-11-634, September 15, 2011)

Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings (GAO-11-565, July 19, 2011)

APPENDIX B: FEDRAMP RECOMMENDED CONTROL-SPECIFIC CONTRACT CLAUSES

No.	Control Specific Area	Description
1	Data Jurisdiction	No NIST SP 800-53 controls govern data location; providers may describe boundaries that include foreign data centers. Agencies with specific data location requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored.
2	FIPS PUB 140-2 Validated Cryptography for Secure Communications	The FedRAMP security control baseline includes IA-7, SC-8(1), SC-9(1), SC-13, and SC-13(1), all of which require cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.
3	2.3. AU-10(5): Non-repudiation	The organizational parameter requires that cloud service providers implement FIPS PUB 140-2 validated cryptography for digital signatures. If the agency has a requirement for integration with specific digital signature technologies, that should be included within the contract requirements.
4	2.4 AU-11: Audit Record Retention	Agencies should consider the length of time they require cloud service providers to retain audit records as part of their contracts with cloud service providers. The FedRAMP requirement is that the service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with National Archives and Records Administration requirements.
5	2.5 IA-2(1), (2), (3) and (8): Identification and Authentication (Organization Users) Multi-Factor Authentication	Cloud service providers pursuing a FedRAMP authorization will have to provide a mechanism for Government consuming end-users to use multi-factor authentication. However, agencies requiring a specific method of authentication, or integration with an existing agency system (such as a SAML 2.0 authentication to the agency's identity provider) must specify this requirement in their contract. In accordance with Department of Homeland Security Presidential Directive 12 (HSPD-12), agencies should consider specific requirements to support Personal Identity Verification/Common Access Card cards.
6	2.6 IA-8: Identification and Authentication (Non-organizational Users)	Cloud service providers pursuing a FedRAMP authorization will have to provide multi-factor authentication for provider's administrators.
7	2.7. IR-6: Incident Reporting Timeframes	FedRAMP parameters set compliance for incident reporting at the levels stipulated in NIST SP 800-61; and the authorizing officials will require an Incident Reporting plan that complies with those requirements. Agency contracts should stipulate any specific incident reporting requirements including who and how to notify the agency.
8	2.8 MP-5(2) and (4): Media Transport	No FedRAMP discussion for this control.

No.	Control Specific Area	Description
9	2.9. PS-3: Personnel Screening	Federal agencies are responsible for the level of Background Investigations that should be conducted in accordance with Office of Personnel Management and OMB requirements. As a note, the Joint Authorization Board does not have contracts with cloud service providers achieving provisional authorizations and therefore does not provide background investigations for cloud service providers seeking a provisional authorization. Agencies leveraging FedRAMP provisional authorizations will be responsible for conducting their own background investigations and/or accepting reciprocity from other agencies that have implemented cloud service provider systems. FedRAMP parameters set reinvestigation parameters as follows: moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth year. There is no reinvestigation for other moderate risk positions or any low risk positions. Agencies are responsible for the screening process and may want to stipulate additional screening requirements.
10	2.10. SC-7(1): Boundary Protection	Cloud service providers pursuing a FedRAMP authorization will have to provide boundary protection in accordance with SC-7; however, if the agency data assets require utilization of a trusted internet connection, the agency must include requirements for data routing within their contract.
11	2.11. SC-28: Protection of Information at Rest	Cloud service providers pursuing a FedRAMP authorization will have to support the capability to encrypt data-at-rest; however, contract clauses should indicate any specific agency requirements for data encryption.
12	2.12. SI-5: Security Alerts, Advisories, and Directives	Cloud service providers are required to include FedRAMP personnel in the list of personnel required to receive alerts, advisories and directives; if an agency elects to include their own security operations center or security personnel in alerts, an agency should include a contract clause.

Source: FedRAMP control specific contract clauses, as of June 2014.

APPENDIX C: ADDITIONAL FEDRAMP REQUIRED CONTROLS AND ENHANCEMENTS

No.	Control ID	Control Name
		FedRAMP Low Security Controls
1	CA-02(01)	Security Assessments: Independent Assessors
		FedRAMP Moderate Security Controls
1	AC-2 (5)	Account Management: Inactivity Logout
2	AC-2 (7)	Account Management: Role-Based Schemes
3	AC-2 (9)	Account Management: Restrictions On Use Of Shared Groups and Accounts
4	AC-2 (10)	Account Management: Shared and Group Account Credential Termination
5	AC-2 (12)	Account Management: Account Monitoring and Atypical Usage
6	AC-4 (21)	Information Flow Enforcement: Physical and Logical Separation Of Information Flows
7	AC-10	Concurrent Session Control
8	AC-17 (9)	Remote Access: Disconnect and Disable Access
9	AU-9 (2)	Protection Of Audit Information: Audit Backup On Separate Physical Systems and Components
10	CA-2 (2)	Security Assessments: Specialized Assessments
11	CA-2 (3)	Security Assessments | External Organizations
12	CA-3 (3)	System Interconnections: Unclassified Non-National Security System Connections
13	CA-8	Penetration Testing
14	CA-8 (1)	Penetration Testing: Independent Penetration Agent Or Team
15	CM-2 (2)	Baseline Configuration: Automation Support For Accuracy and Currency
16	CM-5 (1)	Access Restrictions For Change: Automated Access Enforcement and Auditing
17	CM-5 (3)	Access Restrictions For Change: Signed Components
18	CM-5 (5)	Access Restrictions For Change: Limit Production and Operational Privileges
19	CM-6 (1)	Configuration Settings: Automated Central Management, Application, and Verification
20	CM-7 (5)	Least Functionality: Authorized Software and Whitelisting
21	CM-10 (1)	Software Usage Restrictions: Open Source Software
22	CP-2 (2)	Contingency Plan: Capacity Planning
23	CP-9 (3)	Information System Backup: Separate Storage For Critical Information
24	IA-2 (5)	Identification And Authentication (Organizational Users): Group Authentication
25	IA-4 (4)	Identifier Management: Identify User Status
26	IA-5 (4)	Authenticator Management: Automated Support For Password Strength Determination
27	IA-5 (6)	Authenticator Management: Protection Of Authenticators
28	IA-5 (7)	Authenticator Management: No Embedded Unencrypted Static Authenticators
29	IR-7 (2)	Incident Response Assistance: Coordination With External Providers
30	IR-9	Information Spillage Response
31	IR-9 (1)	Information Spillage Response: Responsible Personnel
32	IR-9 (2)	Information Spillage Response: Training
33	IR-9 (3)	Information Spillage Response: Post-Spill Operations
34	IR-9 (4)	Information Spillage Response: Exposure To Unauthorized Personnel
35	MA-3 (3)	Maintenance Tools: Prevent Unauthorized Removal
36	MA-5 (1)	Maintenance Personnel: Individuals Without Appropriate Access
37	MP-6 (2)	Media Sanitization: Equipment Testing
38	PE-13 (2)	Fire Protection: Suppression Devices and Systems

No.	Control ID	Control Name
39	PE-14 (2)	Temperature And Humidity Controls: Monitoring With Alarms and Notifications
40	PS-3 (3)	Personnel Screening: Information With Special Protection Measures
41	RA-5 (5)	Vulnerability Scanning: Privileged Access
42	RA-5 (6)	Vulnerability Scanning: Automated Trend Analyses
43	RA-5 (8)	Vulnerability Scanning: Review Historic Audit Logs
44	SA-4 (8)	Acquisition Process: Continuous Monitoring Plan
45	SA-9 (2)	External Information Systems: Identification Of Functions, Ports, Protocols, and Services
46	SA-9 (4)	External Information Systems: Consistent Interests Of Consumers And Providers
47	SA-9 (5)	External Information Systems: Processing, Storage, And Service Location
48	SA-10 (1)	Developer Configuration Management: Software and Firmware Integrity Verification
49	SA-11 (1)	Developer Security Testing And Evaluation: Static Code Analysis
50	SA-11 (2)	Developer Security Testing And Evaluation: Threat And Vulnerability Analyses
51	SA-11 (8)	Developer Security Testing And Evaluation: Dynamic Code Analysis
52	SC-6	Resource Availability
53	SC-7 (8)	Boundary Protection: Route Traffic To Authenticated Proxy Servers
54	SC-7 (12)	Boundary Protection: Host-Based Protection
55	SC-7 (13)	Boundary Protection: Isolation Of Security Tools, Mechanisms, and Support Components
56	SC-7 (18)	Boundary Protection: Fail Secure
57	SC-12 (2)	Cryptographic Key Establishment And Management: Symmetric Keys
58	SC-12 (3)	Cryptographic Key Establishment And Management: Asymmetric Keys
59	SC-28 (1)	Protection Of Information At Rest: Cryptographic Protection
60	SI-2 (3)	Flaw Remediation: Time To Remediate Flaws and Benchmarks For Corrective Actions
61	SI-3 (7)	Malicious Code Protection | Nonsignature-Based Detection
62	SI-4 (1)	Information System Monitoring: System-Wide Intrusion Detection System
63	SI-4 (14)	Information System Monitoring: Wireless Intrusion Detection
64	SI-4 (16)	Information System Monitoring: Correlate Monitoring Information
65	SI-4 (23)	Information System Monitoring: Host-Based Devices
66	SI-6	Security Function Verification

Source: FedRAMP "System Security Plan Template v2.0," June 2014.

APPENDIX D: DESCRIPTION OF UNAPPROVED CLOUD COMPUTING SERVICES DISCOVERED BY AGENCY OR IDENTIFIED DURING AUDIT

No.	Cloud Computing Service	Typical Use of Service	Covered by NASA IT Security Plan
1	EC2, S3, IAM, EBS, VPC[a]	Science Information Processing; Web Apps	No
2	Direct Cloud	In use across Agency as replacement for Adobe Reader X	No
3	iCloud	Online service that provides an email account, online storage, and backup services. It also allows the sharing of data between devices, such as Macs, iPhones, and iPads	No
4	Box	Online file storage service that includes multi-user management and collaboration features	No
5	Dropbox	Online storage service that enables users to store files on remote cloud servers and the ability to share files	No
6	Evernote	In use across Agency for note taking, to-do lists	No
7	OneNote	In use across Agency for note taking, to-do lists	No
8	Prezi	In use across Agency for presentations	No
9	AINS, Inc.	Workflow for processing of Freedom of Information Act requests	Yes
10	Hyperoffice	Web-based document collaboration	Yes
11	Medgate, Inc.	Health records management system	Yes
12	Opal	Social-business management (collaboration on social campaigns, exhibits, and press releases)	Yes
13	Airbus Defense and Space	Emergency notification system	Yes
14	PSIwebware, Inc.	Facilities help-desk management system	Yes
15	Icohere	Collaboration Platform	Yes
16	MozyPro	Automatic backup protection with the option to schedule your backups continuously throughout the day.	Yes
17	Foxit Cloud	Document management	No
18	Team Viewer	Collaboration tool, information exchange	No
19	Filecloud	Internal FileCloud instance	Yes
20	Q-KESS	Contractor implemented for work order tracking, etc.	Yes
21	Langley Contract Management System (LCMS)	Contract management system currently used by the Langley IT Enhanced Services II (LITES II) and the Science, Technology, and Research Support Services III (STARSS III) contracts.	Yes
22	CodeLathe: FileCloud	File, sync, and share	No
23	Atlassian:JIRA	Enterprise Content Management	Yes
24	Prevo Technologies: TechDoc	Enterprise Content Management	Yes

No.	Cloud Computing Service	Typical Use of Service	Covered by NASA IT Security Plan
25	IdeaScale	An innovation management platform employing the principles and practices of crowdsourcing. The International Space Station Program uses this service to collect and manage ideas submitted by our employees on potential ways to improve our processes, applications, or facilities.	Yes
26	Survey Monkey	Provides customizable surveys, as well as a suite of back-end programs that include data analysis, sample selection, bias elimination, and data representation tools.	No
27	iTunes	Online tool to organize and enjoy the music, movies, and TV shows you already have. However, it allows for the storage and syncing of document files and photographs.	No
28	Huddle	Project management, sharing and managing documents, coordinating multi-agency projects, and working with external partners.	No

Source: NASA OIG.

[a] The Agency is moving away from use of this service.

APPENDIX E: MANAGEMENT'S COMMENTS

National Aeronautics and Space Administration
Office of the Administrator
Washington, DC 201546-0001

JAN 30 2017

Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report, "Security of NASA's Cloud Computing Services" (A-16-002-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled "Security of NASA's Cloud Computing Services" (A-16-002-00), dated December 21, 2016.

In the draft report, the OIG makes six recommendations addressed to the Chief Information Officer (CIO), intended to strengthen security controls over cloud computing.

Specifically, the OIG recommends the CIO:

Recommendation 1: Monitor adherence to the requirement that only approved cloud computing services on NASA's cloud services registry be used to transmit, process, and store NASA data and block access on NASA networks to unapproved services that do not have an authorization to operate and established information technology (IT) system security plans.

Management's Response: Concur. NASA is deploying a Cloud Access Security Broker (CASB) capability that will perform discovery of cloud services in use on the NASA network. Once an undesirable cloud service is discovered on the NASA network, the domain name and IP address(es) will be provided to the IT security team for blocking via the Agency IT security border protection capabilities.

Estimated Completion Date: January 10, 2018.

Recommendation 2: Ensure NASA personnel at Agency Centers, Mission Directorates, and Program and Project Offices coordinate acquisition of any cloud computing service through the Computing Services Program Office (CSPO) to ensure cloud services are properly accounted for on the Agency's cloud services registry and that all recommended Federal Risk Authorization Management Program (FedRAMP) contract provisions are incorporated into the acquisition.

Management's Response: Concur. NASA will work through the Office of Procurement and the Office of General Counsel to craft a standard set of contract clauses for use when acquiring cloud services.

Estimated Completion Date: September 29, 2017.

Recommendation 3: Ensure NASA's portfolio of approved cloud computing services is sufficient to meet Agency needs.

Management's Response: Concur. NASA is currently revamping its Application Portfolio Management processes to determine if the application portfolio is technically supportable and can deliver the business capabilities needed now and in the future. These processes will ensure that the NASA community understands how to vet new requirements against existing solutions and identify gaps in solutions that must be filled to meet current and future Agency needs. This process work began with the FY16 Annual Capital Investment Review (ACIR) and will continue to evolve with each subsequent ACIR.

Estimated Completion Date: January 31, 2019.

Recommendation 4: Ensure all approved cloud services are registered with FedRAMP and are FedRAMP compliant.

Management's Response: Partially Concur. Although there are nearly 20,000 cloud products available in the marketplace, since the FedRAMP mandate went into effect for Federal agencies in June 2014, less than 100 FedRAMP authorizations have been granted. As a result, "officially" FedRAMP-approved products represent only 0.5 percent of available cloud products. Because so few cloud products have received FedRAMP approval, Federal agencies are inhibited from fully adopting the "cloud first" approach to replacing information technology resources with cloud solutions as directed in the President's digital strategy. NASA will use FedRAMP approved cloud services whenever available. Otherwise, NASA will perform an appropriate risk assessment, and may make a risk-based decision to approve the service for use at NASA, considering mission requirements/impacts, availability of alternative cloud services, information categorization, other industry compliance standards met, and NASA security safeguards that could be employed to ensure safe use.

Estimated Completion Date: September 29, 2017.

Recommendation 5: Incorporate information on the use of and risks associated with cloud computing into required IT security training for all NASA employees.

Management's Response: Concur. NASA will develop a cloud computing chapter for the required annual IT security awareness training.

Estimated Completion Date: September 30, 2018.

Recommendation 6: Direct all NASA Centers, Mission Directorates, and Program and Project Offices to review their current cloud computing services and take steps necessary to ensure that existing services meet FedRAMP requirements.

Management's Response: Concur. The NASA CIO will issue a memorandum to: 1) Direct NASA Centers, Mission Directorates, and Program and Project offices to review their current cloud computing services and take steps necessary to ensure that existing services have been vetted such that they have an Authorization to Operate and that they are part of an approved IT Security plan; and 2) Advise the Agency of the new required procurement guidelines and processes regarding the acquisition of cloud computing.

Estimated Completion Date: January 10, 2018.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have identified information that should not be publicly releasedand have provided that information to the OIG in separate correspondence.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Ruth McWilliams on (202) 358-5125.

Renee P. Wynn FOR

APPENDIX F: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Acting Administrator
Acting Deputy Administrator
Acting Chief of Staff
Chief Information Officer
Assistant Administrator for Procurement
Director, Glenn Research Center
Director, Johnson Space Center

Non-NASA Organizations and Individuals

Office of Management and Budget
    Deputy Associate Director, Energy and Space Programs Division

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 Space, Science, and Competitiveness

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

(Assignment No. A-16-002-00)