United States Department of Agriculture

Office of Inspector General

USDA's Implementation of Cloud Computing Services

50501-0005-12

September 2014

USDA's Implementation of Cloud Computing Services

Audit Report 50501-0005-12

What Were OIG's Objectives

Our objective was to evaluate USDA agencies' efforts to adopt cloud computing technologies and review contracts that agencies have issued for cloud services for compliance with applicable standards.

What OIG Reviewed

We reviewed 6 contracts, with a reported value of approximately $68.5 million, which were selected from a universe of 31 contracts, with an approximate value of $128.2 million. Cloud computing contracts were reviewed for inclusion of detailed specifications and compliance with the June 5, 2014, FedRAMP requirement.

What OIG Recommends

OIG recommends that USDA establish a consistent definition of cloud computing, create and maintain an accurate inventory of its cloud systems, and develop a guide for procuring cloud systems that details specifications and security requirements. The Department also needs a detailed plan for becoming FedRAMP compliant.

OIG reviewed the implementation of commercial cloud computing environments in USDA.

What OIG Found

The Department of Agriculture (USDA) has incorporated cloud computing into its overall information technology (IT) environment, but the Office of Inspector General (OIG) found that the Department does not have a complete inventory of its cloud systems, due to poor inventory management and the inconsistent application of the definition of a cloud computing system. We found that even though USDA has an official system of record for its inventory of IT systems, 17 of the 31 cloud systems were not included in the inventory, and 8 additional systems were in the inventory, but not marked as cloud systems. Additionally, the level of detail included within the contracts for procuring the systems varied across our sample, with all six reviewed contracts lacking details required by Federal guidelines. Finally, only two of the six cloud service providers tested met the requirements to become Federal Risk and Authorization Management Program (FedRAMP) compliant by June 5, 2014.

These issues occurred because the offices and agencies have adopted cloud computing technologies without clear guidance, including a USDA-wide definition of what constitutes a cloud computing system. USDA does not have an adequate process for inventory management, standardized contract language for cloud computing services, and an organized approach to ensure cloud systems meet FedRAMP requirements.

USDA does not have adequate controls in place to manage its cloud service providers and the data that reside in these systems. As a result, USDA's data are exposed to risk of loss or disclosure to unauthorized parties, which could compromise the Department's programs and producer data. Furthermore, because five of six contracts (totaling approximately $66.9 million) did not specify how a provider's performance was to be measured, reported, or enforced, the agencies are not able to ensure adequate service levels are met, increasing the risk that USDA funds could be misspent or ineffectively used.

USDA generally concurred with our findings.

United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

DATE: September 26, 2014

AUDIT NUMBER: 50501-0005-12

TO:

Cheryl Cook
Chief Information Officer
Office of the Chief Information Officer
ATTN: Christopher Wren

Brandon Willis
Administrator
Risk Management Agency
ATTN: Heather Manzano

Lisa Wilusz
Director
Office of Procurement and Property Management
ATTN: Lennetta Elias

Jason Weller
Chief
Natural Resources Conservation Service
ATTN: Leon Brooks

Roger Klurfeld
Director
National Appeals Division
ATTN: Steven Placek

FROM: Gil H. Harden
Assistant Inspector General for Audit

SUBJECT: USDA's Implementation of Cloud Computing Services

This report presents the results of the subject audit. Your written response, dated September 22, 2014, is included in its entirety at the end of the report. Excerpts from your response and the Office of Inspector General's (OIG) position are incorporated in the relevant sections of the report. Based on your written response, we accept management decision on Recommendations 4, 5, 6, and 7. We are unable to accept management decision on Recommendations 1, 2, and 3. The documentation or action needed to reach management decision for these recommendations is described under the relevant OIG Position sections.

In accordance with Departmental Regulation 1720-1, please furnish a consolidated reply, coordinated by the Office of the Chief Information Officer, within 60 days describing the corrective actions taken or planned, and timeframes for implementing the recommendations for which management decisions have not been reached. Please note that the regulation requires management decision to be reached on all recommendations within 6 months from report

issuance, and final action to be taken within 1 year of each management decision to prevent being listed in the Department's annual Agency Financial Report. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions. This report contains publically available information and will be posted in its entirety to our website (http://www.usda.gov/oig) in the near future.

Table of Contents

Background and Objectives 1
Section 1: Cloud Inventory Management 3
Finding 1: USDA Must Develop an Accurate Cloud System Inventory 3
Recommendation 1 4
Recommendation 2 5
Section 2: Cloud Contracting 6
Finding 2: USDA Needs to Include More Detailed Specifications in Its Cloud Contracts 6
Recommendation 3 10
Section 3: FedRAMP Compliance 11
Finding 3: USDA and CSPs Must Meet FedRAMP Requirements 11
Recommendation 4 12
Recommendation 5 12
Recommendation 6 13
Recommendation 7 13
Scope and Methodology 15
Abbreviations 16
Exhibit A: Summary of Monetary Results 17
Agency's Response 19

Background and Objectives

Background

Cloud computing is a term used to define information technology (IT) systems, software, or infrastructure that are packaged and provided to customers by a service provider. The National Institute of Standards and Technology (NIST) describes cloud systems as having five essential components, which are:

- On-demand self-service: The customer is able to unilaterally provision computing capabilities with the service provider, as needed, without requiring human interaction.
- Broad network access: The capabilities (e.g., storage, servers, databases) of the service provider are accessed by the customer through a network connection.
- Resource pooling: The customer shares vendor services with other customers.
- Rapid elasticity: The service provider's system allows the customer to rapidly expand or contract required computing resources.
- Measured service: The customer's payment for use of the cloud system is determined by a measured capability (e.g., seat licenses, storage used).[1]

Cloud computing offers the potential for significant cost savings through more efficient provisioning of computing resources, flexible payments that increase or decrease based on resources needed, and a decreased need to buy hardware or build data centers.

To accelerate the Federal Government's use of cloud-computing strategies, the U.S. Chief Information Officer published the *Federal Cloud Computing Strategy,* requiring agencies to evaluate safe, secure cloud computing options before making any new investments.[2] Due to this "Cloud First" policy, Federal agencies are to evaluate cloud services for new IT projects in an effort to realize the value of cloud computing through cost savings.

In addition to risks that resemble those of in-house information systems, cloud technologies have risks that are unique to the system's deployment. For example, when using a cloud system, the customer relinquishes the ability to govern the system. Specifically, the client cedes control to the cloud service provider (CSP) on a number of issues which may affect the system's security. At the same time, Service Level Agreements (SLA) may not require CSPs to offer such services, thus leaving a gap in security defenses.[3]

---

[1] NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing,* September 2011.
[2] Kundra v. *Federal Cloud Computing Strategy*, February 8, 2011.
[3] European Network and Information Security Agency (ENISA) *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, November 2009.

To effectively manage the delivery of cloud-computing services, agencies should develop contracts that address business and security risks, as well as properly define and provide a mechanism to monitor agency and CSPs' responsibilities. Additionally, agencies must have strong governance practices in place, including organizational control and oversight of policies, procedures, and standards for IT service acquisition and for monitoring the use of cloud services.

In a previous audit, we identified security issues related to cloud computing. Specifically, in the fiscal year 2012 USDA Federal Information Security Management Act (FISMA) report, we recommended that the Office of the Chief Information Officer (OCIO) modify its service agreement between the Department and its e-mail CSP to incorporate appropriate detail, outlining the roles and responsibilities of each party pertaining to incident response and reporting.[4]

Based on the risks surrounding cloud computing, a proposal was submitted by the National Aeronautics and Space Administration OIG to the Council of the Inspectors General on Integrity and Efficiency (CIGIE) for a Government-wide audit initiative on the implementation of cloud computing at Federal agencies. The audit plan was approved by the CIGIE IT Committee and the results from USDA OIG's audit will be consolidated, along with results from other participating OIGs, into a CIGIE report.[5]

Objectives

Our objective was to evaluate USDA agencies' efforts to adopt cloud-computing technologies and review contracts that agencies have issued for cloud services for compliance with applicable standards.

[4] Audit Report 50501-0003-12, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2012Federal Information Security Management Act*, November 2012.
[5] To be released under Audit Report 50501-0007-12.

Section 1: Cloud Inventory Management

Finding 1: USDA Must Develop an Accurate Cloud System Inventory

We determined USDA does not have an inventory that includes all of its cloud systems. More specifically, we found that even though USDA has an official system of record for its inventory of IT systems, 17 of the 31 cloud systems were not included in the inventory, and 8 additional systems were in the inventory, but not marked as cloud systems. This occurred because the Department lacks a sufficient inventory management process and not all agencies were following the NIST definition of cloud computing when designating a system as a cloud system. As a result, the Department does not know the number and type of its cloud systems and associated data that reside outside of USDA information system boundaries, which increases the risk that data could be disclosed to unauthorized parties.

The Office of Management and Budget (OMB) requires Federal agencies to follow NIST guidance.[6] According to NIST, Federal agencies need to develop and document an inventory of information system components that: (1) accurately reflects the current information system, (2) includes all components within the authorization boundary of the information system, and (3) includes the granularity deemed necessary for tracking and reporting.[7]

In addition, an inventory of hardware and an inventory of software are the number one and two controls listed in the Council on Cybersecurity's Critical Security Controls.[8] These two inventories are considered two of the basic controls for building a secure network. The critical controls are a recommended set of actions for cyber defense that provide specific and actionable ways to mitigate the most pervasive attacks. Attackers are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to a network. Therefore it is critical to maintain an asset inventory of all systems connected to the network, including the network devices themselves, and to include every system that has an Internet protocol address on the network. Without an accurate and complete cloud system inventory, agencies cannot ensure the appropriate controls are in place to protect the systems and their data.

According to OCIO, Cyber Security Assessment and Management (CSAM) is the official system of record for the inventory of IT systems within USDA.[9] However, when we began validating the initial inventory of 21 cloud systems that were identified from survey results submitted by

---

[6] OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* November 18, 2013.
[7] NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013.
[8] A consortium of U.S. and international agencies and experts from private industry around the globe contributed to the creation of the Critical Security Controls. They provided recommendations for what ultimately became the Critical Security Controls, which were coordinated through the SANS Institute. In 2013, the stewardship and sustainment of the controls was transferred to the Council on Cyber Security, an independent, global non-profit entity committed to a secure and open Internet.
[9] SOP-ISD-007, *Information Technology Inventory Reconciliation and Certification*, April 28, 2009.

USDA agencies and offices, we identified additional systems that were not reported to us, as well as systems that needed to be removed from the audit universe because they were not consistent with NIST's definition of a cloud system. Once we had established the audit universe of 31 cloud systems, we compared it to CSAM. We found 25 of the 31 identified systems and supporting documentation were not included in CSAM. Due to USDA's inability to provide an accurate inventory of its cloud systems, along with the fact that systems and supporting documentation were missing from CSAM, we have concluded that a complete inventory of USDA cloud systems does not exist. This occurred because the Department lacks a sufficient inventory management process for cloud systems. Although USDA has an inventory management process in place, it relies on agencies to manually report their systems to OCIO for tracking. USDA is a geographically diverse organization with 24 Chief Information Officers (CIO) responsible for the IT management of 34 agencies and staff offices. This decentralized nature of IT management throughout USDA provides challenges with maintaining an accurate and complete inventory. Additionally, USDA has not consistently followed or enforced the NIST definition of cloud computing systems. Our testing determined that agency officials were not adhering to the NIST definition of cloud computing. In effect, agencies were left to make their own determinations on what constitutes a cloud system. Consequently, there is no way to certify that USDA knows of all cloud systems within the Department. In turn, this means that the Department cannot identify all program data that reside in these systems. Without such knowledge, USDA cannot ensure the appropriate controls are in place to protect each system and its data. These risks include isolation failure, interception of data in transit, and insecure/ineffective deletion of data, which could expose agency data to unauthorized parties and potentially compromise the objectives of the agencies' programs.[10]

In conclusion, USDA needs to ensure that it has an accurate and complete inventory of its cloud-based systems.

Recommendation 1

OCIO needs to establish a definition of cloud computing systems for use within USDA that is consistent with NIST guidance.

Agency Response

OCIO accepts this recommendation. OCIO has completed a draft cloud policy that is consistent with NIST guidance, and contains a comprehensive definition of cloud computing systems. The draft is being vetted internally to OCIO for review and comment, prior to being released for formal Department-wide coordination and approval. The estimated completion date is November 30, 2016.

[10] Isolation failure is the risk that the mechanisms used to keep cloud tenants' data separate fail, thus exposing sensitive data to other tenants within the cloud deployment. Intercepting data in transit is the risk that as data are being sent to/from the cloud service, data traffic could be intercepted via sniffing or man-in-the-middle attacks. Insecure/ineffective deletion of data is the risk that once a cloud service contract is terminated, not all data within the cloud can be, or are, securely deleted due to the nature of the data storage within the cloud.

OIG Position

We are unable to reach management decision based on OCIO's response. Although we agree with the issuance of a cloud computing policy, we believe interim measures are needed if the policy will not be ready for publication until November 30, 2016. In order to reach management decision, OCIO needs to provide OIG with interim milestones prior to the proposed publication date of the policy.

Recommendation 2

OCIO needs to create and maintain an accurate cloud system inventory and work with agencies to ensure their adherence to reporting requirements.

Agency Response

OCIO accepts this recommendation. OCIO will collaborate with USDA agencies to review CSP systems in CSAM and develop guidelines as to how CSP systems are to be recorded in CSAM so that future reporting is complete and accurate. The estimated completion date of the CSAM Cloud System Inventory Guide is January 30, 2016.

OIG Position

We are unable to reach management decision based on OCIO's response. Although we agree with the issuance of a CSAM Cloud Inventory Guide, we believe interim measures are needed if the guide will not be ready for publication until January 30, 2016. In order to reach management decision, OCIO needs to provide OIG with interim milestones prior to the proposed publication date of the Cloud Inventory Guide.

Section 2: Cloud Contracting

Finding 2: USDA Needs to Include More Detailed Specifications in Its Cloud Contracts

We found that all six cloud contracts in our sample did not contain detailed specifications for the agency and the cloud service provider (CSP) to adhere to, including detailed Service Loan Agreements (SLA), data preservation responsibilities, roles and responsibilities, Federal regulation requirements, and audit and investigative access for OIG.[11] Although the contracts tested did contain some of the elements, no one contract included all of the elements. This occurred because the Department lacks guidance on a standardized approach to procuring cloud services, including a standard set of requirements for CSPs to adhere to when USDA issues contracts for cloud services. Due to this, USDA has not incorporated adequate service agreements in its cloud service contracts. As a result, USDA has not implemented adequate controls to monitor and manage its CSPs and the data that reside within the systems, exposing USDA data to the risk of loss or exposure to unauthorized parties. Furthermore, because five of six contracts, totaling approximately $66.9 million, did not include detailed SLAs which specify how a provider's performance would be measured, reported, or monitored, the agencies are not able to ensure adequate service levels are met, increasing the risk that Government funds could be misspent or ineffectively used.

NIST recommends that if the terms of the default service agreement do not address all consumer needs, the consumer should discuss modifications of the service agreement with the provider prior to use.[12] In regards to consumer needs, the CIO council and Chief Acquisition Officers (CAO) council's cloud best practices report provides specific guidance on how Federal agencies should effectively procure cloud services within existing regulations and laws.[13] For example, it suggests agencies establish Terms of Service (TOS) agreements that detail how end-users may use the services, the CSP's responsibilities, and how the CSP will deal with customer data. It also recommends Federal agencies require CSPs to allow forensic investigations for both criminal and non-criminal purposes. In addition, the agency and CSP's SLA should have clearly defined terms, definitions, and penalties for failure to meet SLA performance measures. Specific details of our testing follow:

Service Level Agreement (SLA)

The SLA defines the expected level of service to be delivered and, in the event that the CSP fails to deliver the service at the specified level, the service credit available to the cloud consumer.[14] We found five of six cloud contracts reviewed lacked detailed SLAs, which should define the

[11] Data preservation responsibilities address how long the CSP must maintain the agency's data, whether the agency or CSP retains the data ownership rights, and how data are to be sanitized throughout the system lifecycle.
[12] The default service level agreements of public clouds specify limited promises that providers make to subscribers, limit the remedies available to subscribers, and outline subscriber obligations in obtaining such remedies. NIST SP 800-146, *Cloud Computing Synopsis and Recommendations,* May 2012.
[13] The CIO Council and CAO Council guidance, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service,* February 24, 2012.
[14] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing,* December 2011.

required, measurable service levels to be provided by the CSP to the agencies. For example, the required uptime percentage requires the CSP to maintain a level of system availability to the agency for a specified period of time. In regards to uptime percentage, we found that five of six contracts did not specify how a provider's performance would be measured, reported, or monitored, specifically:

- Two of six contracts reviewed did not specify the required uptime percentages for the CSP.

- Three of four contracts that included uptime requirements did not describe how the uptime percentage was calculated. The method for this calculation is critical so that the agency can verify the uptime percentages stated are being met by the CSP.

- Two of four contracts did not detail remedies to be paid by the CSP to the agency if uptime requirements were not met. NIST 800-146 states that if a CSP fails to provide the stated availability, the CSP should compensate consumers in good faith with a service credit for future use of cloud services.

- One of four contracts did not assign someone from the agency to monitor the actual uptime, compare it to the uptime percentage specified in the contract, and pursue service credits when applicable. NIST 800-146 states that the responsibility for obtaining a service credit is generally placed on the consumer, who must provide timely information to the CSP about the nature and the time length of the outage.

In total, these contracts are valued at approximately $66.9 million and have no established method by which to verify that USDA agencies and offices are receiving adequate service levels. By not establishing a method to measure, monitor, and report on the availability of the system, it is possible that USDA funds could be misspent or ineffectively used on poorly performing systems. Without agency monitoring and verification of the uptime percentage, the agency cannot be assured that a service credit will be received if the specified uptime percentage is not met. We consider the development and implementation of a guide for procuring cloud services to be the first step for establishing sufficient cloud services contracts within USDA, which would include the development of detailed SLAs. Based on this, we are not making a recommendation specific to the absence of detailed SLAs in our sampled contracts.

Data Preservation

Data preservation responsibilities should address how long the CSP must maintain the agency's data, whether the agency or CSP retains the data ownership rights, and how data are to be sanitized throughout the system lifecycle.[15] However, for the six contracts reviewed, we found that five did not include data preservation requirements.

[15] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing,* December 2011.

Non-Disclosure Agreements (NDA)

Since CSP personnel have access to and control of the Federal data residing in the cloud system, Non-Disclosure Agreements (NDA) are a critical control to ensure CSPs protect the information being stored in the cloud.[16] However, two of six CSPs did not sign an NDA with the agency in order to protect non-public information that is procurement-sensitive, or affects pre-decisional policy, physical security, or other information deemed important to protect. Of the four agencies that did establish an NDA with the CSP, we found that all four contracts did not establish a method for the agency to monitor end-user activities in the cloud environment.[17] Defining a method for the agency to use for monitoring end-user activities provides the agency with a process to verify adherence to the NDA.

Roles and Responsibilities

In order to effectively manage cloud services, it is essential that roles and responsibilities are clearly defined for the Federal agency, integrators, and the CSP.[18] NIST 800-146 states that an agency should understand both its responsibilities and those of the CSP before using a cloud service. Accordingly, it is important that all terms are agreed to by the CSPs and the agencies to ensure that both parties fully understand their duties when providing and using a cloud service. During our testing, we reviewed the sampled contracts for inclusion of TOS requirements. TOS requirements generally include how end-users may use the services, the responsibilities of the CSP, and how the CSP will deal with customer data. Our review found four of six contracts did not contain TOS specifications.

Federal IT Regulatory Requirements

In addition to contract roles and responsibilities, agencies are subject to unique policy and regulatory requirements. Federal agencies must ensure that any selected cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization.[19] Furthermore, NIST states that the Federal Information Security Management Act (FISMA) and the associated NIST standards and special publications are applicable to cloud systems. However, all six contracts reviewed did not completely address applicable Federal rules and regulations, such as FISMA, OMB Circular A-123, or the Freedom of Information Act.

---

[16] The CIO Council and CAO Council guidance, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service,* February 24, 2012.

[17] The rules of behavior, which are required in OMB Circular A-130, Appendix III, and are a security control contained in NIST SP 800-53, should clearly delineate responsibilities and expected behavior of all individuals with access to the system. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems,* February 2006.

[18] An integrator is an individual or organization that builds systems from a variety of diverse components. With the increasing complexity of technology, more customers want complete solutions to information problems, requiring hardware, software, and networking expertise in a multivendor environment.

[19] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing,* December 2011.

Access to CSP for Audit and Investigative Purposes

OIG offices of audit and investigations must have access to CSP personnel, facilities, and Federal agency information to perform their statutory oversight roles. The CIO council and CAO council's cloud best practices report states that Federal agencies should require CSPs to allow forensic investigations for both criminal and non-criminal purposes, and these investigations should be able to be conducted without affecting data integrity and without interference from the CSP.[20] We reviewed the sampled contracts for the presence of specifications that relate to this type of access.

- All six contracts reviewed did not include language allowing agencies to conduct forensic investigations for both criminal and non-criminal purposes without interference from the CSP.

- All six contracts did not detail procedures for electronic discovery when conducting a criminal investigation.

- All six contracts did not include language to allow OIG full and unrestricted access to the contractors' (and subcontractors') facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews.

Without proper access to the CSP and the services being provided, OIG cannot verify that security controls are in place to reduce risk to a level acceptable to the agency. Additionally, limiting OIG access to CSP facilities and data could compromise and interfere with audits and criminal investigations.

The nature of cloud computing requires customers to cede control to the CSP on a number of issues which may affect security. At the same time, service agreements may not offer or include a commitment from the CSP to provide such services, thus leaving a gap in security defenses.[21] Without detailed contract specifications that include SLAs, data preservation responsibilities, roles and responsibilities, regulation requirements, and audit and investigative access, USDA's data stored in the cloud environment are at risk. Additionally, without the ability to determine how the CSPs' performance is measured, reported, or monitored, USDA does not have the ability to verify service levels are being met, which increases the risk that USDA's funds could be misspent or ineffectively used.

We concluded that it is critical for the Department to develop a consistent approach for cloud system procurements, including guidance on detailed requirements that must be incorporated into contracts.

---

[20] Recognizing this issue, the CIGIE IT Committee drafted clauses that would ensure OIG audit and investigative access and proposed their inclusion in the Federal Acquisition Regulation (FAR) to the FAR Council in January 2012.

[21] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks, and Recommendations for Information Security,* November 2009.

Recommendation 3

OCIO needs to develop and implement a guide for procuring cloud systems that details specifications and security requirements to include in the contracts.

Agency Response

OCIO accepts this recommendation. OCIO has completed a draft guide for procuring cloud system solutions, which contains program solution specifications and security requirements. The guide will be issued to the Office of Procurement and Property Management (OPPM) and agencies for review and comment. The final guide will be issued by OCIO and OPPM for use with USDA information technology cloud system solution procurement contracts. The estimated completion date of the CSAM Cloud System Inventory Guide is November 30, 2016.

OIG Position

We are unable to reach management decision based on OCIO's response. Although we agree with the issuance of a guide for procuring cloud systems, we believe interim measures are needed if the guide will not be ready for publication until November 30, 2016. In order to reach management decision, OCIO needs to provide OIG with interim milestones prior to the proposed publication date of the guide.

Section 3: FedRAMP Compliance

Finding 3: USDA and CSPs Must Meet FedRAMP Requirements

We determined that four of the six reviewed systems were not compliant with the Federal Risk and Authorization Management Program (FedRAMP) by the required deadline of June 5, 2014. The owners of the systems were the Natural Resources Conservation Service (NRCS), OCIO, and the Risk Management Agency (RMA). Ultimately, this occurred because the Department did not establish a comprehensive inventory of all cloud services. FedRAMP states that establishing an inventory of all cloud services within an agency is a critical step on the path to FedRAMP compliance. Once established, the agency needs to work with CSPs to update contractual requirements and determine the path each cloud system will take in order to become FedRAMP compliant. Since the Department did not establish an accurate cloud system inventory, it could not plan accordingly to ensure cloud services properly achieved FedRAMP compliance. CSPs that were non-compliant were in various stages of preparing their FedRAMP certification review packages for submission. FedRAMP's purpose is to ensure that cloud-based services have an adequate information security program that addresses the specific characteristics of cloud computing and provides the level of security necessary to protect Government information. Failure of the cloud system to address and meet FedRAMP security controls increases the risk that USDA program data may be compromised, intercepted, or lost, which could expose the data to unauthorized parties.

FedRAMP was initiated on December 8, 2011, via an OMB policy memo, which addressed the security authorization process for cloud computing services.[22] In the memo, OMB requires each executive department or agency to use FedRAMP when conducting risk assessments, security authorizations, and granting an authority to operate (ATO) for use of cloud services.[23] FedRAMP provides a cost-effective, risk-based approach for the adoption and use of cloud services. It includes:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels.[24]

- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs.

---

[22] S. VanRoekel, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011.

[23] The assessment and authorization process is the new terminology for the former certification and accreditation process mandated by OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (November 28, 2000). The process requires that IT system controls be documented and tested by technical personnel and that the system be given a formal ATO by an agency official before the system can be operated.

[24] The system's security category is determined in accordance with Federal Information Processing Standard 199. After the category is determined, the contractor shall apply the appropriate set of baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance with security standards. The FedRAMP baseline controls are based on NIST SP 800-53, Rev. 4.

- Authorization packages of cloud services reviewed by a Joint Authorization Board consisting of security experts from Department of Homeland Security, Department of Defense, and General Services Administration.[25]

- Standardized contract language to help executive departments and agencies integrate FedRAMP requirements and best practices into acquisitions of cloud systems.

- A repository of authorization packages for cloud services that can be leveraged Government-wide.

Due to the unique risks associated with cloud computing environments, FedRAMP incorporated controls from NIST 800-53 into its baseline security control framework for use with cloud systems. All cloud services currently implemented were required to meet FedRAMP requirements by June 5, 2014.

Without complying with FedRAMP, USDA and its agencies could be facing significant cloud-related security weaknesses that are, as yet, unknown. It is therefore critical that USDA move, in a timely manner, to bring these systems into compliance.

Recommendation 4

OCIO needs to conduct oversight to ensure each agency with cloud services obtains FedRAMP compliance.

Agency Response

OCIO accepts this recommendation. OCIO will provide Department-wide guidance via memorandum to USDA Agencies requiring them to obtain FedRAMP certification of cloud services and will establish an organizational structure to provide oversight to monitor and ensure that USDA agencies cloud services are FedRAMP compliant. The estimated completion date for issuing the Departmental Memorandum on FedRAMP Certification is December 30, 2014, and the estimated completion date for the OCIO FedRAMP Oversight Program is March 30, 2015.

OIG Position

We accept OCIO's management decision.

Recommendation 5

RMA needs to develop a detailed plan to attain FedRAMP compliance for its cloud service that is non-compliant.

[25]Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. A package should include, at a minimum, the security plan, security assessment report, plan of action and milestones, and a continuous monitoring plan.

Agency Response

RMA concurs with the recommendation. RMA is aware that the CSP is pursuing FedRAMP certification by either the Agency Authorization path or the Provisional Authorization Path. USDA is not the Agency Sponsor. RMA will contact the CSP to determine their status on attaining FedRAMP certification. Based on CSP information RMA will develop a detailed plan to track the CSP's progress toward attaining FedRAMP certification. Given that RMA is not the CSP's sponsor, it is not responsible for delays in completing FedRAMP certification but will continuously monitor the progress and update the plan accordingly. The estimated completion date for the plan is November 30, 2014.

OIG Position

We accept RMA's management decision.

Recommendation 6

NRCS needs to develop a detailed plan to attain FedRAMP compliance for its cloud service that is non-compliant.

Agency Response

NRCS concurs with the recommendation. NRCS is aware that the CSP is pursuing FedRAMP certification for the CSP software by the Provisional Authorization Path. NRCS will contact the CSP to determine their status on attaining FedRAMP certification. Based on the response NRCS will track the CSP's progress toward attaining FedRAMP certification. Given that NRCS is not the cloud service provider for the software. NRCS is not responsible for delays in completing FedRAMP certification but will continuously monitor and track the CSP progress accordingly. The estimated completion date for the plan is November 30, 2014.

OIG Position

We accept NRCS' management decision.

Recommendation 7

OCIO needs to develop a detailed plan to attain FedRAMP compliance for its cloud service that is non-compliant.

Agency Response

OCIO concurs with the recommendation. OCIO is the Agency Sponsor for the CSP that is pursuing FedRAMP certification by the Agency Authorization Path. OCIO will work with the CSP to determine their status on attaining FedRAMP certification. OCIO will develop a detailed plan to track the CSP's progress toward attaining FedRAMP certification. OCIO will

continuously monitor the CSP's progress and update the plan accordingly. The estimated completion date for the plan is November 30, 2014.

OIG Position

We accept OCIO's management decision.

Scope and Methodology

This work was conducted to evaluate USDA's efforts to adopt cloud-computing technologies in a manner that complied with current guidance issued by OMB, NIST, and the Department. The documentation includes results from audit tests of a sample of contracts that USDA and its agencies and offices issued for cloud services for compliance with applicable standards.

For this audit, we obtained an inventory of cloud systems. The information was solicited from all agencies and offices within USDA through the use of a survey and did not rely on information derived from any USDA database.

Based on the information obtained, we attempted to validate the survey results by comparing the results with information housed in CSAM, and to USDA's Exhibit 53c submission. We ultimately assembled an audit universe of USDA's cloud systems consisting of 31 contracts, with a value of approximately $128.2 million; however, we cannot be certain that we identified all cloud systems within USDA. Only cloud systems from commercial service providers were included in the universe. From the audit universe, we selected a non-statistical sample of six contracts for detailed testing. The sample, with a total value of $68.5 million, was selected based on a combination of highest dollar value contracts and system risk. Additionally, we reviewed related contract documentation and guidance, and interviewed applicable personnel in order to obtain sufficient and appropriate audit evidence to support our conclusions.

Fieldwork was conducted between January and June, 2014 at applicable agency locations in Washington, D.C.; Albuquerque, New Mexico; Fort Collins, Colorado; and Kansas City, Missouri. In total, our audit work covered four agencies and staff offices:

- NAD
- NRCS
- OCIO, and
- RMA.

We conducted this audit 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Abbreviations

ATO ..... authority to operate
CAO ..... Chief Acquisitions Officers
CIGIE ..... Council of the Inspectors General on Integrity and Efficiency
CIO ..... Chief Information Officer
CSAM ..... Cyber Security Assessment and Management
CSP ..... cloud service provider
ENISA ..... European Network and Information Security Agency
FAR ..... Federal Acquisition Regulation
FedRAMP ..... Federal Risk and Authorization Management Program
FISMA ..... Federal Information Security Management Act
IT ..... information technology
NAD ..... National Appeals Division
NDA ..... non-disclosure agreement
NIST ..... National Institute of Standards and Technology
NRCS ..... Natural Resource Conservation Service
OCIO ..... Office of the Chief Information Officer
OIG ..... Office of Inspector General
OMB ..... Office of Management and Budget
OPPM ..... Office of Procurement and Property Management
RMA ..... Risk Management Agency
SLA ..... service level agreement
SP ..... special publication
TOS ..... terms of service agreements
USDA ..... Department of Agriculture

Exhibit A: Summary of Monetary Results

Exhibit A summarizes the monetary results for our audit report by finding and recommendation number.

Finding	Recommendation	Description	Amount	Category
2	3	CSP Contract Performance Measurement, Reporting, and Monitoring	$66,871,914	Questioned Costs, No Recovery Recommended
Total			$66,871,914	

USDA'S
RESPONSE TO AUDIT REPORT

United States Department of Agriculture

Departmental Management

Office of the Chief Information Officer

1400 Independence Avenue S.W.
Washington, DC 20250

TO: Gil H. Harden
Assistant Inspector General for Audit
Office of Inspector General

FROM: Cheryl L. Cook /s/ Joyce Hunter SEP 19 2014
Chief Information Officer FOR
Office of the Chief Information Officer

Brandon Willis /s/ SEP 22 2014
Administrator
Risk Management Agency

Jason Weller /s/ SEP 19 2014
Chief
Natural Resources Conservation Service

SUBJECT: Response to Official Draft Report, 50501-0005-12, USDA's Implementation of Cloud Computing Services

The Office of the Chief Information Officer (OCIO), the Office of Procurement and Property Management (OPPM), the Risk Management Agency (RMA), and the Natural Resources Conservation Service (NRCS) have reviewed the Official Draft Report, 50501-0005-12, USDA's Implementation of Cloud Computing Services and submit the following response to OIG's recommendations.

Recommendation 1

The Office of the Chief Information Officer (OCIO) needs to establish a definition of cloud computing systems for use within USDA that is consistent with the National Institute of Standards and Technology (NIST) guidance.

Agency Response: OCIO accepts this recommendation. OCIO has completed a draft cloud policy that is consistent with NIST guidance, and contains a comprehensive definition of cloud computing systems. The draft is being vetted internally to OCIO for review and comment, prior to being released for formal Department-wide coordination and approval

- Departmental Regulation on Cloud Computing Policy
  Target Completion Date: November 30, 2016

Recommendation 2

OCIO needs to create and maintain an accurate cloud system inventory and work with agencies to ensure their adherence to reporting requirements.

Agency Response: OCIO accepts this recommendation. OCIO will collaborate with USDA agencies to review CSP systems in CSAM and develop guidelines as to how CSP systems are to be recorded in CSAM so that future reporting is complete and accurate.

- CSAM Cloud System Inventory Guide
  Target Completion Date: January 30, 2016

Recommendation 3

OCIO needs to develop and implement a guide for procuring cloud systems that details specifications and security requirements to include in the contracts.

Agency Response: OCIO accepts this recommendation. OCIO has completed a draft guide for procuring cloud system solutions, which contains program solution specifications and security requirements. The guide will be issued to OPPM and agencies for review and comment. The final guide will be issued by OCIO and OPPM for use with USDA information technology cloud system solution procurement contracts.

- Departmental Regulation on Cloud Computing Policy
  Target Completion Date: November 30, 2016

Recommendation 4

The Office of the Chief Information Officer (OCIO) needs to conduct oversight to ensure each agency with cloud services obtain Federal Risk and Authorization Management Program (FedRAMP) compliance.

Agency Response: OCIO accepts this recommendation. OCIO will provide Department-wide guidance via memorandum to USDA Agencies requiring them to obtain FedRAMP certification of cloud services and will establish an organizational structure to provide oversight to monitor and ensure that USDA agencies cloud services are FedRAMP compliant.

- Departmental Memorandum on FedRAMP Certification
  Target Completion Date: December 30, 2014

- OCIO FedRAMP Oversight Program
  Target Completion Date: March 30, 2015

Recommendation 5

The Risk Management Agency (RMA) needs to develop a detailed plan to attain

FedRAMP compliance for its cloud service that is non-compliant.

Agency Response: RMA concurs with the recommendation. RMA is aware that the CSP is pursuing FedRAMP certification by either the Agency Authorization path or the Provisional Authorization Path. USDA is not the Agency Sponsor. RMA will contact the CSP to determine their status on attaining FedRAMP certification. Based on CSP information RMA will develop a detailed plan to track the CSP's progress toward attaining FedRAMP certification. Given that RMA is not the CSP's sponsor, it is not responsible for delays in completing FedRAMP certification but will continuously monitor the progress and update the plan accordingly.

- **RMA CSP FedRAMP Certification Tracking Plan**

  Target Completion Date: November 30, 2014

Recommendation 6

The Natural Resources Conservation Service (NRCS) needs to develop a detailed plan to attain FedRAMP compliance for its cloud service that is non-compliant.

Agency Response: NRCS concurs with the recommendation. NRCS is aware that Pega Systems is pursuing FedRAMP certification for the PEGA software by the Provisional Authorization Path. NRCS will contact Pega Systems to determine their status on attaining FedRAMP certification. Based on Pega Systems response NRCS will track PEGA's progress toward attaining FedRAMP certification. Given that NRCS is not the cloud service provider for PEGA software. NRCS is not responsible for delays in completing FedRAMP certification but will continuously monitor and track Pega Systems progress accordingly.

- **NRCS CSP FedRAMP Certification Tracking Plan**
  Target Completion Date: November 30, 2014

Recommendation 7

OCIO needs to develop a detailed plan to attain FedRAMP compliance for its cloud service that is non-compliant.

Agency Response: OCIO concurs with the recommendation. OCIO is the Agency Sponsor for the CSP that is pursuing FedRAMP certification by the Agency Authorization Path. OCIO will work with the CSP to determine their status on attaining FedRAMP certification. OCIO will develop a detailed plan to track the CSP's progress toward attaining FedRAMP certification. OCIO will continuously monitor the CSP's progress and update the plan accordingly.

- **OCIO CSP FedRAMP Certification Tracking Plan**

  Target Completion Date: November 30, 2014

cc: Jane Bannon, Program Manager, OIG
Christopher Wren, OCIO Audit Liaison
Lennetta Elias, OCFO Audit Liaison

To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste and Abuse
e-mail: USDA.HOTLINE@oig.usda.gov
phone: 800-424-9121
fax: 202-690-2474

Bribes or Gratuities
202-720-7257 (24 hours a day)

The U.S. Department of Agriculture (USDA) prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex (including gender identity and expression), marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD).

To file a complaint of discrimination, write to USDA, Assistant Secretary for Civil Rights, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, S.W., Stop 9410, Washington, DC 20250-9410, or call toll-free at (866) 632-9992 (English) or (800) 877-8339 (TDD) or (866) 377-8642 (English Federal-relay) or (800) 845-6136 (Spanish Federal relay).USDA is an equal opportunity provider and employer.