



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Management of Cloud Computing Contracts and Environment

Audit Report

Report Number
IT-AR-14-009

September 4, 2014





OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Highlights

***Cloud computing contracts
did not comply with
Postal Service standards.***

Background

The Council of Inspectors General on Integrity and Efficiency asked inspectors general in the federal community to participate in an audit of cloud computing contracts. Cloud computing provides on-demand network access to shared resources that can be rapidly released and allows customers to take advantage of cutting edge technologies at a reduced cost. Hosted services are offered by providers that host physical servers in a different location. The audit was designed to provide insight on how well the federal government is protecting data and its progress in moving towards cloud computing.

As a participant in this audit, our objectives were to determine if the U.S. Postal Service's cloud service contracts comply with applicable standards and evaluate management's efforts to adopt cloud computing technologies.

What the OIG Found

The Postal Service's cloud computing contracts did not comply with all applicable Postal Service's standards. Specifically, the Postal Service has not defined "cloud computing" and "hosted services," established an enterprise-wide inventory of cloud computing services, required suppliers and their employees to sign non-disclosure agreements, or included all required information security clauses in its contracts.

In addition, management did not appropriately monitor applications to ensure system availability. Management also did not complete the required security analysis process for three cloud services reviewed and did not follow Postal Service policy requiring cloud service providers to meet federal government guidelines. This occurred because no group is responsible for managing cloud services, and personnel were not aware of all policy and contractual obligations.

Without proper knowledge of and control over applications in the cloud environment, the Postal Service cannot properly secure cloud computing technologies and is at increased risk of unauthorized access and disclosure of sensitive data. We claimed \$33,517,151 in contractual costs for the Postal Service not following their policy and contract requirements.

What the OIG Recommended

We recommended management define "cloud computing" and "hosted services," develop an inventory of cloud services, monitor suppliers and require them to be certified, and revise contracts to include security clauses. We also recommended management evaluate best practices for cloud computing contracts, complete the security analysis process, and ensure compliance with non-disclosure clauses.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 4, 2014

MEMORANDUM FOR: JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

SUSAN M. BROWNELL
VICE PRESIDENT, SUPPLY MANAGEMENT

CHARLES L. MCGANN
MANAGER, CORPORATE INFORMATION SECURITY

A rectangular box containing a handwritten signature in black ink that reads "John E. Cihota". There is a small black dot in the upper right corner of the box.

FROM: John E. Cihota
Deputy Assistant Inspector General
for Finance and Supply Management

SUBJECT: Audit Report – Management of Cloud Computing Contracts and Environment (Report Number IT-AR-14-009)

This report presents the results of our audit of the Management of Cloud Computing Contracts and Environment (Project Number 14BG007IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean Balduff, deputy director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Cover	1
Highlights	1
Background	1
What the OIG Found	1
What the OIG Recommended	1
Transmittal Letter	2
Findings	4
Introduction	4
Conclusion	5
Defining and Managing the Cloud Services Environment	6
Defining Cloud Computing and Hosted Services	6
Cloud Computing Enterprise-Wide Inventory	6
Monitoring of Applications	7
Contract Management	8
Information Security Contract Clauses	8
Best Practices for Cloud Computing Contracts	9
Non-Disclosure Agreements	10
Compliance with the Federal Risk and Authorization Management Program and the Certification and Accreditation Process	10
Recommendations	11
Management's Comments	12
Evaluation of Management's Comments	13
Appendices	14
Appendix A: Additional Information	15
Background	15
Objective, Scope, and Methodology	15
Prior Audit Coverage	17
Appendix B: Management's Comments	18
Contact Information	24

Findings

Introduction

This report presents the results of our audit of the Management of Cloud Computing Contracts and Environment (Project Number 14BG007IT000). The Council of Inspectors General on Integrity and Efficiency (CIGIE)¹ Information Technology (IT) Committee² asked IGs to participate in an audit of their agency's cloud computing contracts. The information will be consolidated to determine how well the federal government is protecting data in the cloud environment and its progress in moving towards cloud computing technologies. Our objective was to determine if the U.S. Postal Service's cloud service contracts comply with applicable standards and evaluate management's efforts to adopt cloud computing technologies. See [Appendix A](#) for additional information about this audit.

The Office of Management and Budget's (OMB)³ "Cloud First" policy⁴ requires federal agencies to default to cloud-based solutions whenever there is a secure, reliable, and cost-effective cloud option. Effectively procuring and managing cloud computing services requires agencies to develop contracts that address business and security risks, as well as properly define and provide a mechanism to monitor agency and cloud service providers' (CSP)⁵ responsibilities.



- 1 An independent entity that addresses integrity, economy, and effectiveness issues that transcend individual government agencies; and increases the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid the offices of inspectors general.
- 2 The CIGIE IT committee facilitates effective IT audits, evaluations, and investigations by inspectors general (IG) and provides a vehicle for the IG community to express its perspective on government-wide IT operations.
- 3 The OMB is the largest component of the Executive Office, reporting directly to the president and helping a wide range of executive departments and agencies across the federal government implement the commitments and priorities of the president.
- 4 *25 Point Implementation Plan to Reform Federal Information Technology Management*, dated December 9, 2010.
- 5 A person, organization, or entity responsible for making a service available to consumers.

The Postal Service has not defined “cloud computing” and does not have an inventory of cloud computing services.

Cloud computing means different things to different people; however, CIGIE uses the National Institute of Standards and Technology’s (NIST)⁶ definition.⁷ The NIST defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources⁸ that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

The Federal Risk and Authorization Management Program (FedRAMP) enables federal agencies to manage service providers that enable cloud computing capabilities. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is the result of the close collaboration of security and cloud experts from the NIST, the OMB, the Department of Defense, the Federal Chief Information Officer Council, and other federal agencies, as well as private industry. By providing a standardized approach, FedRAMP is designed to save money, time, and staff required to assess and authorize cloud services while ensuring adequate information security.

The Postal Service developed a cloud security policy⁹ that requires its CSPs to be FedRAMP-certified and lists the characteristics of cloud computing. These characteristics include on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization.

Conclusion

The Postal Service’s cloud computing contracts did not comply with all of the Postal Service’s applicable standards. While the Postal Service has made progress towards adopting cloud computing technologies, opportunities exist to strengthen its cloud computing contract compliance with Postal Service standards and best practices. Specifically, the Postal Service has not:

- Clearly defined the terms “cloud computing” or “hosted services.”¹⁰
- Established an enterprise-wide inventory of cloud computing services.
- Required the supplier and their employees with access to Postal Service data to sign non-disclosure agreements.
- Included all required information security clauses in its cloud computing contracts.

These steps have not been taken because there is no single group responsible for managing cloud services. In addition, Supply Management personnel believed the contracting officer (CO) had the discretion to waive the non-disclosure requirement. By assessing and implementing cloud computing best practices, the Postal Service will protect its data from security threats and help ensure its integrity and confidentiality. We claimed \$33,517,151 in contractual costs for the Postal Service not following their policy and contract requirements. Some required security clauses were not included in the contracts we reviewed and the Postal Service did not require suppliers and their employees to sign non-disclosure agreements.

⁶ A non-regulatory federal agency in the U.S. Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

⁷ NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, dated September 2011.

⁸ Includes networks, servers, storage, applications, and services.

⁹ Handbook AS-805-H, *Cloud Security*, dated August 2013.

¹⁰ Hosted services are outsourced IT systems and functions offered by a provider that hosts the physical servers running that service somewhere else. Access to the service is usually provided through a direct network connection or via the Internet.

In addition, in four contracts we reviewed we found that, while management assigned personnel to monitor the cloud services, they did not appropriately monitor the cloud service applications to ensure service level agreements (SLA)¹¹ were performed or recognize applicable service credits.¹² Also, the Postal Service did not require CSPs to become FedRAMP-certified, as required, or complete the Certification and Accreditation (C&A)¹³ process because personnel were not aware of all of the contractual obligations or the Postal Service's cloud computing requirements.

By requiring CSPs to become FedRAMP-certified, the Postal Service can leverage a standardized baseline of security controls and ensure cloud services are continuously monitored. In addition, requiring CSPs to complete the C&A process on Postal Service cloud computing applications mitigates the risk of a sensitive data breach.

Defining and Managing the Cloud Services Environment

The Postal Service is not effectively managing cloud computing services, applications, and contracts. Specifically, it has not defined "cloud computing" and "hosted services." In addition, it does not have an enterprise-wide inventory of cloud computing services and contracts. Without proper knowledge and control of the cloud environment, the Postal Service cannot properly secure cloud computing technologies and is at risk of unauthorized access to and disclosure of sensitive data.

Defining Cloud Computing and Hosted Services

The Postal Service has not clearly defined the terms "cloud computing" and "hosted services," provided guidance on identifying and classifying cloud computing technologies, or listed detailed roles and responsibilities related to managing these technologies in its policy.¹⁴ Rather, the policy¹⁵ provides an overview of cloud computing initiatives and lists general roles and responsibilities; therefore, management and personnel in various functional areas have different interpretations of cloud computing and its associated capabilities. Since cloud computing is an emerging technology, the Postal Service has not prioritized developing detailed guidance defining "cloud computing" and "hosted services," identifying and classifying cloud computing technologies, and defining roles and responsibilities for managing cloud computing technologies. Without effective management of cloud computing technologies, the Postal Service cannot properly govern and assess the risk associated with these technologies.

Cloud Computing Enterprise-Wide Inventory

The Postal Service does not have an enterprise-wide inventory of cloud computing services that includes the name of the service, CSP, deployment model,¹⁶ service model,¹⁷ and contract number, as required by policy.¹⁸ There is not a single group responsible for managing

11 The SLA provides the quality of service parameters, monitoring, and enforcement according to defined policies. They usually cover availability, scheduled outages, remedies for failure to perform, and service agreement changes.

12 Service credits are amounts deducted from charges payable to the supplier under the contract based on the duration of cloud service outages.

13 A formal security analysis and management approval process to assess residual risk before putting a resource into production.

14 Handbook AS-805-H.

15 Handbook AS-805-H.

16 There are four major cloud computing deployment models: Private Cloud - used by a single organization; Community Cloud - used by a specific community of consumers from organizations with shared concerns, such as a shared mission; Public Cloud - used by the general public; and Hybrid Cloud - a composition of two or more distinct cloud infrastructures such as private, community, or public.

17 There are three major cloud computing service models: Software as a Service - the capability provided to the consumer to use the CSP's applications running on a cloud infrastructure; Platform as a Service - the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider; and Infrastructure as a Service - the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

18 Handbook AS-805, *Information Security*, Section 10-4.7, Maintaining Inventories, dated May 2013.

cloud services, including developing and maintaining an inventory of all cloud services. As a result, the Postal Service cannot effectively manage its cloud computing technologies and ensure the accountability and security of those technologies.

We reviewed the Contract Authoring and Management System (CAMS)¹⁹ and the Enterprise Information Repository (EIR),²⁰ which are the official systems of record for detailed information on Postal Service contracts and applications, and found no field reporting tool to identify cloud computing services or contracts or any readily available information. We attempted to develop a list of cloud computing services; however, knowledge of cloud computing services and contracts is dispersed among various groups, and the Postal Service's IT and Supply Management groups did not always agree on which applications were cloud services.

During our audit, Postal Service management developed Management Instruction AS-800-2014-4, *Cloud Computing Policy*, dated June 2014; however, the policy had not been issued as of August 7, 2014. This policy will define cloud computing, lists roles and responsibilities, and provides cloud computing procedures.

Monitoring of Applications

Postal Service management did not appropriately monitor the [REDACTED]²¹ and [REDACTED]²² applications to ensure system availability and uptime percentages are met as required by the contract award package²³ and policy.²⁴ While management assigned personnel to monitor these two applications, they did not require a review and comparison of the applications uptime percentages to required availability percentages in the SLAs to recognize applicable service credits. For example, personnel responsible for monitoring the [REDACTED] application tracked outages using Remedy²⁵ and developed outage reports based on information within Remedy. However, these reports did not contain specific details for [REDACTED] outages such as start time, end time, and outage duration.

Personnel responsible for monitoring [REDACTED] manually tracked high impact outages²⁶ using emails from the CSP. But they did not maintain reports for all outages or reports containing uptime percentages of the application. In addition, management did not ensure the supplier for [REDACTED] complied with all contractual obligations. For example, while the Postal Service issued Letters of Adequate Assurance²⁷ to [REDACTED] supplier for significant system performance issues, it did not pursue service credits based on the supplier's failure to meet uptime requirements. Also, [REDACTED] experienced four major outages where management did not calculate the actual service credits using the SLA requirements.

19 Provides Supply Management personnel with a web-based application to facilitate the solicitation, award, and administration of supplies, services, and transportation contracts.

20 Provides a centralized storage and access location for standard corporate information resources.

21 A cloud-based solution that handles customer concerns, issues, and complaints; and supports the end-to-end process of initiating, routing, resolving, communicating, and managing customer service requests.

22 A software as a service used to collect, store, and provide reporting on email and other electronic information used in litigation or for other internal Postal Service needs.

23 The contract award package provides all procedures, evaluation techniques, records of negotiation, and the best value determination that must be formally documented and maintained in the contract file. The specific contract file documentation includes the requirements document, approved requisition, purchase plan, Statement of Work (SOW), evaluation documentation, contract award, award notification, and other documentation considered material for award purposes.

24 Handbook AS-805-H, Section 6-2.14, Availability of Postal Service Applications and Information; and Section 7-1, Contract Clauses; and *Supplying Principles and Practices*, Section 2-16.7, Considerations for Using a Performance-Based-Contract; and Section 3-6.12, Contracting Officer Representatives, dated September 2013.

25 The problem tracking and reporting system that support organizations use to keep track of customer-reported problems or requests.

26 Outages that affect multiple users.

27 A written demand for adequate assurance is issued to a supplier for failure to maintain satisfactory performance under the contract and gives the supplier a specified timeframe to assure the Postal Service corrective measures are being taken to address the issue.

These issues occurred because personnel did not use an automated mechanism such as the Enterprise System Monitoring (ESM)²⁸ tools to adequately monitor the availability of [REDACTED] and [REDACTED] applications. In addition, personnel responsible for monitoring these applications were not aware of the requirements associated with the supplier's contractual obligations, maintaining availability reports such as uptime percentages of applications and detailed outages, and recognizing service credits. The Postal Service needs to adequately monitor applications so it can measure the supplier's performance, ensure achievement of agreed-upon service, and recognize applicable service credits.

During this audit, the Postal Service began receiving and maintaining availability reports for the [REDACTED] application; therefore, we are not making a recommendation regarding monitoring and maintaining availability reports for [REDACTED].

Contract Management

Postal Service management did not ensure the supplier's compliance with all contractual obligations as required by policy.²⁹ Specifically, management did not include information security clauses³⁰ in one of the four contracts we reviewed. In addition, cloud computing contract clauses in these four contracts did not specifically address investigative, forensic, and audit access. Also, management did not require the supplier and its employees with access to Postal Service information to sign non-disclosure agreements in accordance with Postal Service cloud service contracts.

As a result, the Postal Service's cloud computing environment is at increased risk of unauthorized access, use, disclosure, and modification. We claimed \$33,517,151 in contractual costs for the Postal Service not following its policy and contract requirements. Some required security clauses were not included in the contracts we reviewed, and the Postal Service did not require suppliers and their employees to sign non-disclosure agreements.

Information Security Contract Clauses

The Postal Service did not include Clause 4-19, Information Security Requirements,³¹ in the [REDACTED] contract as required by policy.³² Clause 4-19 requires suppliers to comply with policies in Handbooks AS-805 and AS-805-A,³³ cooperate with the Postal Service in completing the application Business Impact Assessment to identify the sensitivity and criticality of the application, determine and comply with information security requirements, and mitigate all security vulnerabilities identified during site security reviews. The CO only included a reference to Handbook AS-805 and not the entire Clause 4-19. Without information security contract clauses, the Postal Service's data is at increased risk of potential exposure and a security breach.

In addition, one of the four contracts we reviewed was awarded after Handbook AS-805-H, *Cloud Security*, was established. But the contract did not include language requiring the CSP to comply with Handbook AS-805-H. This occurred because Supply Management has not developed contracting language for including Handbook AS-805-H.

28 Provides standardized monitoring and reporting services and manages systems used for monitoring Postal Service web sites (internal and external facing).

29 *Supplying Principles and Practices*, Section 5-7.1.3, Performance Indicators; Section 5-7.2, QAP and Examination; and Section 6-2.12, CORS.

30 Clause 4-19, Information Security Requirements.

31 *Supplying Principles and Practices* contains clauses and provisions that are required to be included in contracts. Clause 4-19 should be in all contracts relating to IT and information gathering.

32 *Supplying Principles and Practices*, Section 8-4.10, Clauses.

33 Handbook AS-805-A, *Information Resource Certification and Accreditation Process*, dated April 2012.

The U.S. Postal Service Office of Inspector General (OIG) recently issued a report³⁴ regarding cloud computing contracting clauses that noted the Postal Service included language in 13 cloud computing contracts³⁵ to address privacy concerns; however, the contracts did not adequately address information accessibility and data security for network access and server locations. The OIG recommended the Postal Service include requirements from Handbook AS-805 and Handbook AS-805-H in future cloud computing contracts regardless of data sensitivity; therefore, we will not issue a recommendation regarding this issue.

Best Practices for Cloud Computing Contracts

The Postal Service's cloud computing contracts did not completely address the Postal Service's and OIG's access to CSP facilities or investigative, forensic, or audit access. We benchmarked the Postal Service's contract clauses with those of other federal agencies. We found the Postal Service's contract clauses did not address best practices recommended by the NIST, the Chief Information Officers and Chief Acquisition Officers councils, and the Federal Acquisition Regulation (FAR). For example, the contract clauses did not completely address the following:

- Allow the Postal Service access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.
- Allow the Postal Service to conduct forensic investigations for both criminal and non-criminal purposes without interference from the CSP.
- Allow the CSP to only change the cloud environment under specific standard operating procedures agreed to by the CSP and the Postal Service.
- Require contractors to fully cooperate with law enforcement by disclosing sufficient information to identify the nature and extent of an offense, as well as provide timely responses to government auditors' and investigators' requests for documents and access to employees.
- Address procedures for electronic discovery³⁶ when conducting a criminal investigation.
- Grant the OIG access to examine those contractor or subcontractor records pertaining to and involving transactions relating to the contract or subcontract and interview any officer or employee regarding such transactions.
- Allow the OIG full and free access to the contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used to conduct audits, inspections, investigations, or other reviews.

Supply Management was not familiar with specific cloud computing contract clauses or best practice clauses to address investigative, forensic, and audit access. Without cloud computing best practice clauses, the Postal Service's cloud computing environment is at increased risk of unauthorized access, use, and modification.

³⁴ *Cloud Computing Contract Clauses* (Report Number SM-MA-14-005, dated April 30, 2014).

³⁵ Only one of the contracts we reviewed [REDACTED] was in this listing of 13 contracts.

³⁶ The process of locating, preserving, collecting, processing, reviewing, and producing electronically stored information in the context of civil litigation or investigation.

Non-Disclosure Agreements

Of the four contracts we reviewed, only one supplier signed a non-disclosure agreement required by its contract.³⁷ In addition, the signed agreement did not require all employees with access to Postal Service data to sign non-disclosure agreements. Supply Management personnel believed the CO had the discretion to waive this requirement and deemed completion of security clearances by key supplier personnel dealing with Postal Service data sufficient to meet this contractual requirement. As a result, suppliers and their employees may not be aware of or adhering to nondisclosure requirements, placing sensitive Postal Service information at risk of unauthorized disclosure.

Compliance with the Federal Risk and Authorization Management Program and the Certification and Accreditation Process

The Postal Service's CSPs for [REDACTED], [REDACTED], and [REDACTED]³⁸ are not FedRAMP-certified nor have they initiated the process to become FedRAMP-certified. Also, the Postal Service deployed all three of the applications in our sample prior to completing the C&A process. Specifically, the Corporate Information Security Office (CISO) issued a letter stating the [REDACTED] is not compliant with Handbook AS-805 and Payment Card Industry Data Security Standards (PCI DSS)³⁹ due to outstanding security deficiencies. The CISO also issued a letter for the [REDACTED] application stating that adequate security controls and processes have not been implemented and the application is not compliant with Handbook AS-805. However, management has not mitigated or accepted the identified risks for [REDACTED] and [REDACTED] to complete the C&A process. In addition, the [REDACTED] application was deployed into production, but the CSP has not completed the required C&A documentation.

Policy⁴⁰ requires CSPs to become FedRAMP-certified and work with the Postal Service to certify and accredit that the service being provided follows the Postal Service's Information Security C&A process. Postal Service personnel were not aware FedRAMP certification was a requirement and did not require completion of C&A documentation prior to deploying the applications. Without adequate security controls and processes in place, the Postal Service's cloud applications that store sensitive data are at increased risk of a potential security breach.

37 Postal Service Contract Clause 1-1(b)(2), Privacy Protection, Use, Ownership, and Nondisclosure, explicitly states the supplier must restrict access to such information to those employees who need the information to perform work under the contract and ensure that these employees, including subcontractors' employees, sign non-disclosure agreements in a form suitable to the CO, prior to being granted access to the information.

38 [REDACTED] delivers a cloud-based enterprise platform for digital experience marketing called the Distributed Engagement Channel (DEC). DEC is used to create, distribute, and measure dynamic brand experiences across multiple sites and devices on a global scale, such as YouTube.

39 PCI DSS provides a framework for developing a robust payment card data security process including prevention, detection, and appropriate reaction to security incidents.

40 Handbook AS 805-H, Section 6-2.1, Cloud Security Providers; and Section 6-2.8, Certification and Accreditation; and Handbook AS-805, Section 8-4, Certification and Accreditation.

Recommendations

We recommend management define “cloud computing” and “hosted services,” develop an inventory of cloud services, monitor suppliers and require them to be certified, and revise contracts to include security clauses.

Recommendations

We recommend the vice president, Information Technology, in coordination with the manager, Corporate Information Security:

1. Implement an enterprise-wide definition of cloud computing and hosted services, guidance on identifying and classifying cloud computing technologies, and detailed roles and responsibilities for managing cloud computing technologies.

We recommend the vice president, Information Technology, in coordination with the vice president, Supply Management, and manager, Corporate Information Security:

2. Assign a group the responsibility for managing cloud services, including establishing and maintaining an enterprise-wide inventory of all cloud computing technologies.

We recommend the vice president, Information Technology:

3. Evaluate automated monitoring capabilities, such as the Enterprise System Monitoring tools, to determine their feasibility to monitor the availability of Postal Service cloud applications.

We recommend the vice president, Supply Management, in coordination with the vice president, Information Technology:

4. Monitor the [REDACTED] supplier to ensure compliance with all contractual obligations, including service level agreements, and recognize any applicable service credits. Also, develop and maintain availability reports such as uptime percentages of the application and detailed outage reports for the [REDACTED].

We recommend the vice president, Supply Management:

5. Direct contracting officers to include all appropriate information technology clauses in Postal Service cloud computing contracts, revise the [REDACTED] contract to include Clause 4-19, Information Security Requirements, and comply with the requirement that all suppliers and their employees sign nondisclosure agreements.

We recommend the vice president, Supply Management, in coordination with the vice president, Information Technology, and manager, Corporate Information Security:

6. Evaluate best practices for cloud computing contract clauses that address investigative, forensic, and audit access for incorporation into existing and future cloud computing contracts.
7. Require cloud service providers of current and future cloud computing contracts to become Federal Risk and Authorization Management Program-certified in accordance with Postal Service policy.

We recommend the vice president, Information Technology, in coordination with the manager, Corporate Information Security:

8. Complete the Certification and Accreditation process to either accept or mitigate the risks for the [REDACTED], [REDACTED], and [REDACTED] applications.

Management's Comments

Management agreed with the intent of the findings and all of the recommendations except for recommendation 7, to which they partially agreed. Management stated they have recognized the need to address issues surrounding cloud computing services and drafted a handbook on cloud computing policy. Further, management noted that the [REDACTED] and [REDACTED] applications were "hosted services," not "cloud services," conflicting with what was discussed with the Postal Service during the audit. As a result, management believes the financial risk noted by the OIG was inaccurate.

Regarding recommendation 1, management agreed to update Handbooks AS-805 and AS-805-H, and to publish Management Instruction AS-800-2014-4, to provide clarity on cloud computing and hosted services, including definitions, roles, and responsibilities. The target implementation date is October 31, 2014.

Regarding recommendation 2, management agreed to assign a single group responsibility for managing cloud services and maintaining an enterprise-wide inventory of all cloud computing technologies. The target implementation date is December 31, 2014.

Regarding recommendation 3, management agreed to evaluate automated monitoring capabilities to monitor cloud applications. The target implementation date is March 31, 2015.

Regarding recommendation 4, management agreed to ensure supplier compliance and determine whether service credits are due to the Postal Service. The target implementation date is December 31, 2014.

Regarding recommendation 5, management agreed to issue a communication to all COs regarding the requirement to include all appropriate information technology clauses in cloud computing contracts. Management also agreed to include Clause 4-19, *Information Security Requirements*, in the [REDACTED] contract and require supplier level certification and non-disclosure agreements. The target implementation date is January 31, 2015.

Regarding recommendation 6, management agreed to evaluate best practices to determine if it would be in the best interest of the Postal Service to modify its existing contract clauses. The target implementation date is February 28, 2015.

Regarding recommendation 7, management agreed to perform an assessment of existing cloud computing contracts to determine the capability, risk, and associated costs of FedRAMP certification. Management agreed to follow policy requirements for FedRAMP certification for future cloud computing contracts. The target implementation date is February 28, 2015.

Regarding recommendation 8, management agreed to complete the certification and accreditation process for each cited application. The target implementation date is December 31, 2014.

See [Appendix B](#) for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report. While management partially agreed with recommendation 7, the OIG considers management's alternate action to be responsive. Regarding management's comments on the assessment of financial risk, the OIG assessed this risk based on the requirements included in the applications' contracts, not on whether the application was classified as a "cloud service" or a "hosted service."

The OIG considers recommendations 1, 2, 5, 7, and 8 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

Appendices

***Click on the appendix title
to the right to navigate to
the section content.***

Appendix A: Additional Information	15
Background	15
Objective, Scope, and Methodology.....	15
Prior Audit Coverage	17
Appendix B: Management’s Comments.....	18

Appendix A: Additional Information

Background

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources⁴¹ that can be rapidly provisioned and released with minimal management effort or CSP interaction. Cloud computing means different things to different people and determining the appropriate cloud computing environment is essential. Cloud computing offers a unique opportunity for federal agencies and public and private companies to take advantage of cutting-edge information technologies to reduce procurement and operating costs and increase the efficiency and effectiveness of services provided to their customers. Specifically, cloud computing enables organizations to purchase a broad range of IT services and only pay for services as they are used and increase capacity levels without investing in new systems, training new personnel, or licensing new software. This way of doing business allows cloud service providers to offer access to services “in the cloud” through a web browser (over the Internet) while storing business software, infrastructure, and government data on remote servers and, in some cases, with hardware and software owned by the cloud service provider.

FedRAMP enables federal agencies to manage service providers that enable cloud computing capabilities. It is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that will save the money, time, and staff required to conduct redundant agency security assessments. FedRAMP helps ensure that those cloud-based services used government-wide provide adequate information security, eliminates duplicate efforts, reduces risk and cost, and enables rapid and cost-effective procurement of applications and services for federal agencies.

The Postal Service is committed to creating and maintaining an environment that protects its information resources from unauthorized access, use, disclosure, disruption, modification, or destruction to help ensure integrity, confidentiality, and availability. While aspects of cloud characteristics have been realized, cloud computing remains a “work in progress.” Cloud computing leverages economies of scale and balances resources among CSPs. These CSPs provide the cloud computing services specified in their contracts to meet the Postal Service’s operational and security concerns. The Postal Service’s policy requires its CSPs to become FedRAMP-certified, ensuring there is adequate information security. It is important to review standard contract clauses because of the nature of cloud computing. Because the cloud can be used to outsource critical internal infrastructure and the interruption of that infrastructure may have wide-ranging effects, contracts should address data protection, security, privacy, storage locations, and transfer; law enforcement access; confidentiality; and non-disclosure. The cloud computing environment must protect information resources critical to the Postal Service and the privacy of its employees and customers; comply with applicable standards; and assign responsibilities for governance to Postal Service officers, executives, managers, employees, contractors, partners, and vendors.

Objective, Scope, and Methodology

Our objectives were to determine if the Postal Service’s cloud service contracts comply with applicable standards and evaluate management’s efforts at adopting cloud computing technologies.

To accomplish our objectives, we reviewed policies, procedures, and practices for cloud computing governance and security. We met with a contractor who has expertise in the cloud computing field and federal agencies to identify cloud computing best practices and policies. We also reviewed private industry (Fortune 500 companies) standards for benchmarking purposes. We requested cloud computing inventories of all Postal Service cloud services, applications, providers, and contracts from

⁴¹ For example, networks, servers, storage, applications, and services.

Postal Service senior management and personnel within the Supply Management, IT, the CISO, Product Information, and other business units. We received listings of cloud services and contracts, as well as documentation related to the cloud service from several Postal Service officials based on their knowledge of cloud computing services, contracts, and applications. Based on the listings and documentation we received, we piecemealed the information into a listing of 25 cloud services with their corresponding application, CSP, cloud model and type, contract number, and other contract-related information.

To determine our sample, we reviewed the listing for cloud services; applications associated with the services; cloud deployment and service models; sensitivity and criticality levels; whether the application maintained personally identifiable information; and the contract value. We interviewed Supply Management, IT, business owners, and CISO personnel responsible for cloud services to obtain background information on the applications and contracts to develop our sample selection to ensure agreement among all parties on the application's role as a cloud service. We judgmentally selected a sample of four cloud computing contracts for three cloud applications for review: two [REDACTED] contracts, one [REDACTED] contract, and one [REDACTED] contract valued at about \$33,517,151.

We requested contract information from these groups for each cloud service and reviewed the CAMS and EIR for contract file information. Based on our survey results, we performed a detailed evaluation of supporting documentation for the four cloud service contracts to include contract modifications, signed solicitation agreements, requests for proposals, SOWs, purchase plans, terms of service, SLAs, technical requirements, award determinations, non-disclosure agreements, performance reports, FedRAMP compliance, and cloud computing C&A documentation. Based on our review of the contract file documentation, we interviewed Postal Service managers and contracting personnel responsible for the cloud services to determine whether cloud service contracts clearly defined the responsibilities of all parties; defined performance in clear terms; identified how performance will be measured, reported, and enforced; and determined how they monitored the cloud computing providers and services. We used the results of our review to determine areas within the Postal Service cloud computing environment that warrant additional improvement in appropriately governing and securing cloud resources.

We conducted this performance audit from January through September 2014, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on August 7, 2014, and included their comments where appropriate.

We assessed the reliability of the cloud computing inventory data by interviewing Postal Service officials and reviewing the cloud computing systems in the EIR and CAMS. We determined that the data were not sufficiently reliable for the purposes of this report and we made a recommendation regarding this finding.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact (in millions)
<i>Cloud Computing Contract Clauses</i>	SM-MA-14-005	4/30/2014	None
<p>Report Results: The audit concluded that 13 Postal Service cloud computing contracts did not address information accessibility and data security for network access and server location. Postal Service officials also exempted a cloud supplier from following certain policies because the contract did not contain sensitive data. Contracting officials expressed concerns that including the policy in existing cloud computing contracts could increase contract cost. Management generally agreed with the recommendations, all of which we considered significant.</p>			
<i>Availability of Critical Applications</i>	IT-AR-13-008	9/25/2013	None
<p>Report Results: The audit concluded that the Postal Service is proactive in monitoring the Facility Access and Shipment Tracking, PostalOne!-Business Customer Support System, and usps.com applications to ensure they meet established availability targets and updates processes for incident, change, and availability data. However, the Postal Service was not effective in ensuring its Point-of-Service (POS) retail terminal operations, considered a critical application, met availability targets. Employees are not following policy, performing real-time monitoring of POS terminals, determining the duration of outages to ensure availability targets are met, or maintaining availability reports. Management did not agree with the majority of the recommendations, all of which we considered significant.</p>			
<i>U.S. Postal Service Cloud Computing</i>	IT-AR-12-006	5/9/2012	\$5,300,000
<p>Report Results: The audit concluded that opportunities exist for the Postal Service to use cloud computing technologies to support IT operations, resources, and infrastructure. However, no overarching adoption strategies exist to determine which cloud deployment and service models are best suited for current IT operations and resources. Specifically, the Postal Service does not have a consistent strategy or approach for determining the risks and benefits of implementing cloud computing technologies. Management agreed with the recommendations, one of which was considered significant.</p>			
<i>Additional Guidance Needed to Address Cloud Computing Concerns</i>	GAO-12-130T	10/6/2011	None
<p>Report Results: The audit concluded that cloud computing has both positive and negative information security implications for federal agencies. Potential information security benefits include: the use of automation to expedite secure configurations on devices, broad network access, and low-cost disaster recovery and data storage. However, 22 of 24 major federal agencies reported they were either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include dependence on security practices and assurance of vendors and sharing of computing resources. Many agencies also had concerns about vendor compliance and implementation of government information security requirements. Recommendations were not issued for management action.</p>			

Appendix B: Management's Comments



August 27, 2014

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS (A)

SUBJECT: Response to Draft Report - CIGIE Cloud Computing Initiative (IT-AR-14-DRAFT)

Overall, Postal Service management agrees with the intent of Office of Inspector General's (OIG) audit report. Cloud computing services, which is rapidly evolving in the marketplace, presents challenges regarding establishing effective definitions, standards, and policies. Postal Service management recognized the need to address the issues around cloud computing services and drafted Handbook AS-805-H, *Cloud Security* and Management Instruction AS-800-2014-4, *Cloud Computing Policy*, which was shared with the auditors. The audit report does not adequately recognize the efforts of Postal Service management related to cloud activities.

Additionally, while the OIG worked with various Postal Service employees to determine cloud applications, the [REDACTED] and [REDACTED] applications were erroneously classified as "cloud services", when they were actually "hosted services." Therefore, the financial risk noted by the OIG is inaccurate.

Recommendation [1]:

Implement an enterprise-wide definition of cloud computing and hosted services, guidance on identifying and classifying cloud computing technologies, and detailed roles and responsibilities for managing cloud computing technologies.

Management Response/Action Plan:

Management agrees with this recommendation. Work on this effort is underway with regard to updating Handbook AS-805, *Information Systems*; Handbook AS-805-H, *Cloud Security*, and publishing of the *Cloud Computing Policy* Management Instruction (AS-800-2014-4 issued July 2014).

Target Implementation Date:

October 31, 2014

Responsible Officials:

Manager, Solution Development & Support, Information Technology
Manager, Performance Achievement, Information Technology
Manager, Corporate Information Security

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-5000
WWW.USPS.COM

Recommendation [2]:

Assign a group the responsibility for managing cloud services, including establishing and maintaining an enterprise-wide inventory of all cloud computing technologies.

Management Response/Action Plan:

Management agrees with this recommendation. Management has assigned a single group responsible for the management of Postal Service cloud services, as well as providing the ability to maintain an enterprise-wide inventory of all cloud computing technologies. The capability to identify systems utilizing Cloud technologies was added to the Information Technology Enterprise Information Repository (EIR) in July 2014, and will be maintained by Business Relationship Management, Information Technology.

Target Implementation Date:

December 31, 2014

Responsible Official:

Manager, Performance Achievement, Information Technology
Manager, Corporate Information Security

Recommendation [3]:

Evaluate automated monitoring capabilities, such as the Enterprise System Monitoring tools, to determine their feasibility to monitor the availability of Postal Service cloud applications.

Management Response/Action Plan:

Management agrees with this recommendation. Management will evaluate automated monitoring capabilities to monitor Postal Service cloud applications.

Target Implementation Date:

March 31, 2015

Responsible Official:

Manager, Performance Achievement, Information Technology

Recommendation [4]:

Monitor the [REDACTED] supplier to ensure compliance with all contractual obligations, including service level agreements, and recognize any applicable service credits. Also, develop and maintain availability reports such as uptime percentages of the application and detailed outage reports for the [REDACTED]

Management Response/Action Plan:

Management agrees with this recommendation. Management will ensure supplier compliance and determine whether service credits are due to the Postal Service.

Target Implementation Date:

December 31, 2014

Responsible Official:

Manager, Information Technology Software, Services and Retail Category Management Center,
Supply Management
Manager, Performance Achievement, Information Technology
Manager, Business Relationship Management, Information Technology

Recommendation [5]:

Direct contracting officers to include all appropriate information technology clauses in Postal Service cloud computing contracts, revise the [REDACTED] contract to include Clause 4-19, *Information Security Requirements*, and comply with the requirement that all suppliers and their employees sign nondisclosure agreements.

Management Response/Action Plan:

Management agrees with this recommendation. Management will issue a communication to all Contracting Officers detailing the requirement to include the appropriate information technology clauses in cloud computing contracts. Also, Management agrees with including Clause 4-19, *Information Security Requirements*, into the [REDACTED] contract. Management agrees to require supplier level certification and nondisclosure agreements. The intent of Clause 1-1, *Privacy Protection*, is to comply with the Privacy Act (5 U.S.C. 522a) and Postal Service regulations at 39 C.F.R. Parts 266-267. By virtue of including this clause in the contract, the supplier must comply with its requirements. As stated in Clause 1-1 *Privacy Protection b. Customer or Employee Information, 2. Use, Ownership, and Nondisclosure*, the supplier must restrict access to certain information to those employees who need the information to perform work under this contract, and must ensure that each such employee (including subcontractors' employees) sign a nondisclosure agreement, in a form suitable to the contracting officer, prior to being granted access to the information.

Target Implementation Date:

January 31, 2015

Responsible Official:

Manager, Supply Management Infrastructure, Supply Management
Manager, Information Technology Software, Services and Retail Category Management Center
Supply Management

Recommendation [6]:

Evaluate best practices for cloud computing contract clauses that address investigative, forensic, and audit access for incorporation into existing and future cloud computing contracts.

Management Response/Action Plan:

Management agrees with this recommendation. Supply Management will evaluate best practices to determine if it would be in the best interest of the Postal Service to modify our existing contract clause coverage. Management notes that *Clause 4-2: Contract Terms and Conditions Required to Implement Policies, Statutes or Executive Orders (July 2014), b. Examination of Records*, currently included in all contracts, allows for broad investigative, forensic, and audit access to supplier information and data.

Target Implementation Date:

February 28, 2015

Responsible Official:

Manager, Supply Management Infrastructure, Supply Management
Manager, Performance Achievement, Information Technology
Manager, Corporate Information Security

Recommendation [7]:

Require cloud service providers of current and future cloud computing contracts to become Federal Risk and Authorization Management Program (FedRAMP)-certified in accordance with Postal Service policy.

Management Response/Action Plan:

Management partially agrees with this recommendation. For current cloud computing contracts in which FedRAMP certification was not part of the initial requirements because they were solicited prior to policy implementation, an assessment will be performed to determine capability, risk, and associated costs. Implementation would be on a case-by-case basis and in accordance with Postal Service policy documenting any exceptions. Future cloud computing contracts will follow the policy requirements within Handbooks AS-805, *Information Security*; and AS-805-H, *Cloud Security*, for FedRAMP certification.

Target Implementation Date:

February 28, 2015

Responsible Official:

Manager, Technology Infrastructure Portfolio, Supply Management
Manager, Performance Achievement, Information Technology
Manager, Solutions Development & Support, Information Technology
Manager, Corporate Information Security

Recommendation [8]:

Complete the Certification and Accreditation process to either accept or mitigate the risks for the [REDACTED] and [REDACTED] applications.

Management Response/Action Plan:

Management agrees with this recommendation. The Certification and Accreditation process will be completed for each of the cited applications.

Target Implementation Date:

December 31, 2014

Responsible Official:

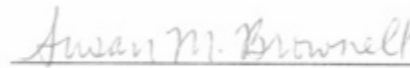
Manager, Business Relationship Management, Information Technology
Manager, Corporate Information Security

FOIA Statement:

This report does contain information which management believes may be proprietary or other business information that may be exempt from disclosure under the Freedom of Information Act (FOIA). Exemption information will be provided separately.



for John T. Edgar
Vice President, Information Technology



Susan M. Brownell
Vice President, Supply Management



2014.08.27

11:03:33 -04'00'

Charles L. McGann
Manager, Corporate Information Security

cc: Sally K. Haring, Manager, Corporate Audit and Response Management



FOIA Exemption information.

The Postal Service requests that all references to the named applications throughout the report and our management response be redacted for security purposes.

Exemption 1 (5 USC 552(b)(1)) — National Defense and Foreign Relations may apply or

Exemption 3 (5 USC 552(b)(3)) — Federal Law. 39 U.S.C. 410(c)(2) Information of a commercial nature, including trade secrets, whether or not obtained from a person outside the Postal Service, which under good business practice would not be disclosed.

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-5000
WWW.USPS.COM



Contact us via our [Hotline](#) and [FOIA](#) forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100