OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Software Contract and Compliance Review

Audit Report

Report Number
IT-AR-15-009

September 18, 2015

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

The software contract did not comply with all applicable standards and management did not ensure the supplier adhered to all contract clauses.

Background

In response to a 2014 cyber intrusion, the U.S. Postal Service purchased [redacted] software through an existing contract with [redacted]. Personnel working on remediation efforts used [redacted] for secure communications after discovering the intrusion compromised Postal Service email servers.

Our objectives were to determine whether the Postal Service's contract for [redacted] software complied with applicable standards and evaluate management's adherence to the contract.

What The OIG Found

The [redacted] software contract did not comply with all applicable standards and management did not ensure the supplier adhered to all contract clauses. Specifically, the Postal Service did not include provisions in the software contract for system integrity, computing environment, and application information security. In addition, the Postal Service did not ensure the supplier complied with all information security requirements, such as storing Postal Service information in a private cloud and becoming Federal Risk and Authorization Management Program-certified. Finally, the Postal Service did not perform a Certification and Accreditation of the software.

The Postal Service also lacks a retention policy specifying how long to maintain emails, sufficient access controls, and a method to ensure that personnel with access to the software have appropriate security clearances. These issues occurred because the original contracting officer was unaware of some provisions that should be in the contract and because management focused on cyber intrusion remediation plans rather than the software and its associated cloud storage security requirements.

Without proper security, contractual, retention, and access controls, the Postal Service is at an increased risk of unauthorized access and disclosure of sensitive information. We questioned about $22 million in contractual costs because the Postal Service failed to complete the Certification and Accreditation process and incorporate required contract provisions.

What The OIG Recommended

We recommended management include all appropriate provisions in their contract and require the supplier to comply with specific security standards and become Federal Risk and Authorization Management Program-certified. We also recommended management complete the Certification and Accreditation process for [redacted] software, develop an email retention policy, and assign personnel to manage access to the software and obtain required security clearances.

Transmittal Letter

Office of Inspector General
United States Postal Service

September 18, 2015

MEMORANDUM FOR: JUDITH A. ADAMS
ACTING VICE PRESIDENT, INFORMATION TECHNOLOGY

GREGORY S. CRABB
ACTING CHIEF INFORMATION SECURITY OFFICER AND
DIGITAL SOLUTIONS VICE PRESIDENT

SUSAN M. BROWNELL
VICE PRESIDENT, SUPPLY MANAGEMENT

E-Signed by Michael Thompson
ERIFY authenticity with eSign Deskto

FROM: Michael L. Thompson
Acting Deputy Assistant Inspector General
for Technology, Investment, and Cost

SUBJECT: Audit Report – [redacted] Software Contract and Compliance Review (Report Number IT-AR-15-009)

This report presents the results of our audit of the [redacted] Software Contract and Compliance Review (Project Number 15TG027IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Cover
Highlights 1
  Background 1
  What The OIG Found 1
  What The OIG Recommended 1
Transmittal Letter 2
Findings 4
  Introduction 4
  Summary 4
  Compliance with Information Security Requirements 5
  Information Security Provisions 6
  Retention Management Policy 6
  Access Controls 7
  Security Clearances 8
Recommendations 9
  Management's Comments 9
  Evaluation of Management's Comments 10
Appendices 11
  Appendix A: Additional Information 12
    Background 12
    Objectives, Scope, and Methodology 12
    Prior Audit Coverage 14
  Appendix B: Management's Comments 15
Contact Information 19

Findings

The Postal Service did not ensure the supplier complied with all information security requirements. For instance, the Postal Service did not perform a Certification and Accreditation of the software.

Introduction

This report presents the results of our audit of the [redacted] software contract and compliance (Project Number 15TG027IT000). Our objectives were to determine if the U.S. Postal Service's contract for the [redacted] software complied with applicable standards and evaluate management's adherence to the contract. See Appendix A for additional information about this audit.

In October 2014, the Postal Service became aware of a cyber intrusion that compromised current and former employee information, customer complaints, and injury claim data. Since that time, the Postal Service has been actively engaged in investigating, remediating, and implementing security enhancements with the goal of managing its network and preventing future attacks.

When the cyber intrusion occurred, the Postal Service determined the perpetrators compromised their exchange servers and could view its emails; therefore, management purchased [redacted] software tenant[1] – [redacted][2] to allow personnel working on the cyber intrusion remediation efforts to securely communicate with one another. The Postal Service also purchased a second [redacted] software tenant – [redacted][3] to allow secure communication among Postal Service managers. The Postal Service purchased both tenants through their existing contract with [redacted].[4]

Summary

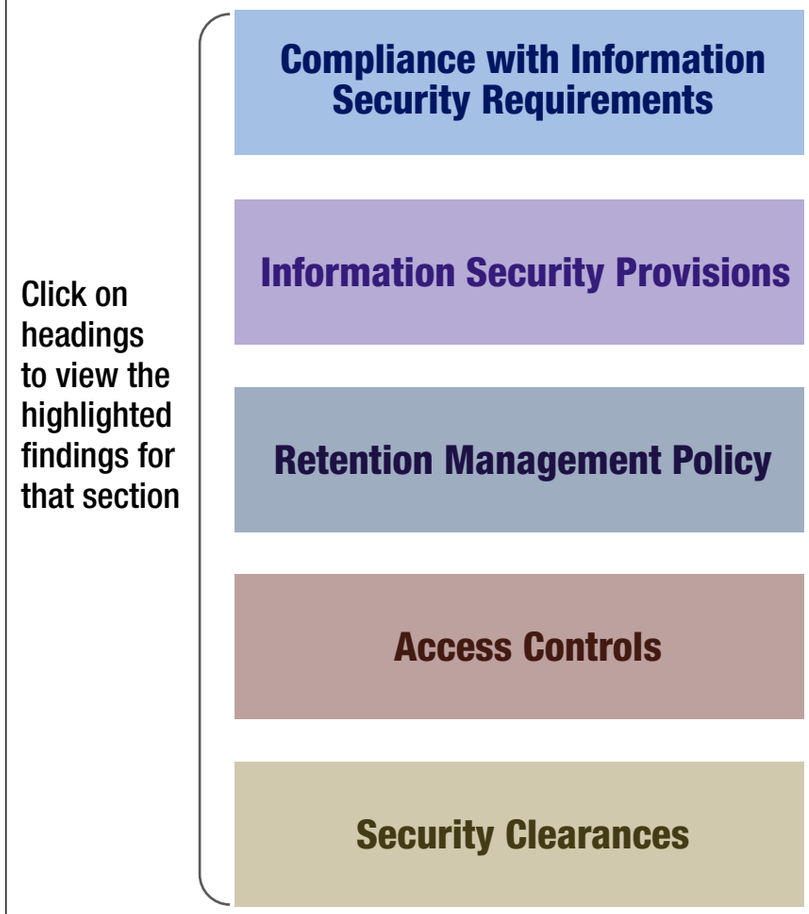
[redacted] and its associated [redacted] software contract did not comply with all applicable standards and management did not ensure the supplier adhered to all clauses in the contract. Specifically, the Postal Service did not include all of the required provisions in the contract. In addition, the Postal Service did not ensure the supplier complied with all information security requirements, such as storing Postal Service information in a secure private cloud and becoming [redacted][5]-certified.[6] The Postal Service also did not perform a Certification and Accreditation (C&A) of the software. In addition, the Postal Service does not have a retention management policy specifying how long emails should be maintained or sufficient access controls in place for the software. Further, some personnel with access to the software did not have the appropriate security clearance. (See Figure 1 for an overview of the findings.)

These issues occurred because the original contracting officer (CO) was unaware of all provisions that should be in the contract and management focused on cyber intrusion remediation plans rather than ensuring the software and its associated cloud storage met security requirements or assigning responsibility for managing access to the [redacted] software. In addition, management was not aware that email timeframes were missing from their policy. Without proper security, contractual, retention, and access controls, the Postal Service is at an increased risk of unauthorized access and disclosure of sensitive information.

By complying with information security requirements and establishing contractual, retention, and access controls, the Postal Service could protect its data from security threats and help ensure its confidentiality and integrity. We claimed about $22 million in contractual costs due to the Postal Service's failure to complete the C&A process and include all required contract provisions in the [redacted] and [redacted] software contract.

1 A dedicated instance that an organization receives and owns when it signs up for a [redacted] cloud service, such as [redacted].
2 [redacted] is an Enterprise version of [redacted] that is stored in a public cloud.
3 [redacted] is a government version of [redacted] that is stored in a hybrid cloud.
4 [redacted] is the third-party vendor that sells software owned by various companies including [redacted]. The Postal Service has to go through this vendor to purchase any software they need.
5 [redacted] is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
6 To become [redacted]-certified a cloud provider must identify, implement, and document security controls and have a third-party assessor verify and validate that these security controls have been implemented.

Figure 1: Overview of Findings



Compliance with Information Security Requirements

The Postal Service did not ensure the supplier complied with all information security requirements as required by their contract[7] and policy.[8] Specifically:

- Postal Service employees and contractors are communicating and storing sensitive and critical information regarding the cyber intrusion remediation efforts in [redacted] – [redacted], which has not been [redacted]-certified. In addition, the Postal Service data in [redacted] are being maintained inappropriately in a public cloud.[9] Policy[10] states that sensitive information must not be deployed to a public cloud and cloud providers must be [redacted]-certified.

- For [redacted], the Postal Service did not review or obtain the [redacted] package and allowed data to be inappropriately stored in a hybrid cloud.[11] Policy[12] states that sensitive information must not be deployed to a hybrid cloud. Hybrid clouds are acceptable only for non-sensitive and non-critical information.

7 [redacted], Contract Number [redacted] Privacy Protection and Clause 4-19, Information Security Requirements, dated October 31, 2014.
8 Handbook AS-805-H, *Cloud Security*, Section 6-1, Cloud Providers and Security, Section 6-2.2, Cloud Initiatives, Section 6-4, Postal Service Applications and Information, and Section 6-9, Infrastructure and Application Assessment and Authorization, dated May 27, 2015.
9 A public cloud is provisioned for open use by the public and exists on the premises of the cloud provider.
10 Handbook AS-805-H, Section 6-1, Cloud Providers and Security, and Section 6-4, Postal Service Applications and Information.
11 A hybrid cloud is a composition of two or more distinct cloud infrastructures (e.g., private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology.
12 Handbook AS-805-H, Section 6-4, Postal Service Applications and Information.

The Postal Service did not include all of the required provisions in the contract. Specifically, the contract did not include Provision 4-6, System Integrity; Provision 4-7, Postal Computing Environment; and Provision 4-10, Application Information Security Requirements.

- The Corporate Information Security Office (CISO) has not performed the C&A process for [redacted] software. In addition, management did not work with the supplier to develop and implement a Business Impact Assessment (BIA) or security plan to protect Postal Service information. Policy[13] states that cloud providers must work with the Postal Service to obtain a C&A. In addition, the [redacted] contract requires suppliers to work with the Postal Service to develop and implement a BIA and security plan and comply with all information security requirements.

- The Postal Service does not know the physical location of [redacted] software emails and data. Policy[14] states that each cloud initiative must have a document containing the location of the Postal Service's data.

During the cyber intrusion, the Postal Service had to expedite its process to implement a secure method for personnel working on remediation efforts to communicate with one another. However, 8 months after the intrusion, management is still working on the remediation efforts and has not made it a priority to ensure the software and its associated cloud storage met the Postal Service security requirements. The lack of adequate security controls and processes increases the risk of a security breach affecting sensitive data.

Information Security Provisions

The Postal Service did not include all of the required provisions in the [redacted] and [redacted] contract. Specifically, the contract did not include Provision 4-6, System Integrity;[15] Provision 4-7, Postal Computing Environment;[16] and Provision 4-10, Application Information Security Requirements.[17]

Postal Service policy[18] requires these provisions to be in third-party software contracts and all solicitations for Information Technology (IT) work that involves generating or collecting sensitive information. The original CO was unaware of all the IT provisions and clauses that should be included in IT and software contracts. As a result, the Postal Service does not have any contractual remedy from the supplier if there is unauthorized use, modification, or disclosure of their information.

Retention Management Policy

The Postal Service does not have a retention management policy specifying timeframes for maintaining emails. Management Instruction AS 870-2011-5[19] establishes policy, standards, and guidelines for electronic messaging, including emails, and states that Postal Service managers are responsible for ensuring appropriate retention of emails. However, the policy does not include any email retention timeframes. Retention periods are also published in the Postal Service's Electronic Record Information Management System (eRIMS);[20] however, eRIMS does not include retention periods for emails. Best practices[21] suggest maintaining emails for senior management permanently and emails for other officials and contractors for 7 years.

---

13 Handbook AS-805-H, Section 6-9, Infrastructure and Application Assessment and Authorization.
14 Handbook AS-805-H, Section 6-2. Cloud Initiatives.
15 This provision requires third-party software vendors to provide a statement certifying their software will not compromise the integrity of the operating system or provide the software source code to ensure the integrity of the Postal Service's computer operating systems.
16 This provision requires all IT infrastructure components and applications to be compliant with the specifications in Handbook AS-820, *Postal Computing Environment.*
17 This provision requires the supplier to comply with policies in Handbook AS-805, *Information Security*, and processes defined in Handbook AS-805-A, *Information Resource Certification and Accreditation Process*.
18 *Supplying Principles and Practices*, Section 8-4.9, Solicitation Provisions, dated February 1, 2015.
19 Management Instruction AS 870-2011-5, *Electronic Messaging*, pages 1 and 4, dated September 2011.
20 eRIMS keeps track of and manages retention schedules for Postal Service forms and data.
21 National Archives and Records Administration, *White Paper on The Capstone Approach and Capstone General Records Schedule (GRS)*, Appendix A: The Capstone GRS, dated April 2015.

This occurred because Postal Service management was not aware the email timeframes were missing from the policy and eRIMS. The Postal Service needs adequate controls to retain key information it may need in the future to protect their infrastructure or records of key decisions made during remediation efforts.

Access Controls

The Postal Service does not have adequate controls to request, authorize, terminate, and review access over [redacted] software – [redacted] and [redacted]. Specifically:

- Employees and contractors did not request access to [redacted] – [redacted] and [redacted] through eAccess[22] or complete Postal Service (PS) Form 1357, Request for Computer Access. Instead, administrators received an email or text message from management and then established a user account.

- Administrators were not terminating access to the software for users who no longer needed it. We reviewed 99 accounts and identified four Postal Service employees and six contractors who no longer worked for the Postal Service but still had access to the software.

- Management did not review the software access list to ensure that it disabled user accounts that were not accessed within 90 days. Specifically, on June 12, 2015, we reviewed all 99 [redacted] – [redacted] accounts and found that 41 of those users (41 percent) had not accessed their account within 90 days. In addition, on July 1, 2015, we reviewed all 137 [redacted] – [redacted] accounts and found that 113 of those users (82 percent) had not accessed their account in 90 days.

- Management created one shared account called Demo User in [redacted] – [redacted] and one shared account called John Doe in [redacted] – [redacted], giving anyone who used these accounts access to sensitive information. During our audit, the Postal Service deactivated these two shared accounts; therefore, we will not make a recommendation regarding these accounts.

Postal Service policy[23] states that all requests for authorization to access Postal Service information resources must be made through eAccess or a PS Form 1357. Managers must make sure to immediately revoke access to information resources for personnel who no longer require it due to a change in job responsibilities. In addition, managers must review access granted to personnel under their supervision at least semiannually and disable accounts that are unused after 90 days.

These access issues occurred because management focused on the cyber intrusion remediation and did not assign personnel responsibility for managing access to the [redacted] software, including requesting, authorizing, terminating, and reviewing access. As a result, the Postal Service's sensitive and critical information regarding their cyber intrusion efforts is at risk of exposure to unauthorized personnel.

22 eAccess is the Postal Service's intranet portal for requesting Postal Service applications and resources.
23 Handbook AS-805, *Information Security,* Section 9-3.2.1, Requesting Authorization, Section 9-3.1.2, Need to Know, Section 9-3.2.5, Periodic Review of Access Authorization, Section 9-3.2.7, Revoking Access, Section 9-4.3, Account Management, Section 9-4.2.4, Shared Accounts, and Section 9-3.2.10, Special Account Registration Management.

We reviewed security clearances for all Postal Service employees and contractors with access to the software on June 24, 2015, and found that 20 of 99 employees (20 percent) did not have appropriate security clearances.

Security Clearances

We reviewed security clearances for all Postal Service employees and contractors with access to [redacted] – [redacted] on June 24, 2015, and found that 20 of 99 employees (20 percent) did not have appropriate security clearances. Specifically:

- Four Postal Service employees did not have a security clearance.
- One Postal Service employee had an expired security clearance. Management renewed the employee's clearance on June 25, 2015, after we brought this issue to their attention.
- Nine contractors did not have a security clearance and two others were in the process of obtaining a clearance after receiving access to [redacted]. In addition, four other contractors obtained a security clearance in May and June of 2015, after they were granted access to [redacted].

Postal Service policy[24] states that all employees who require access to Postal Service information resources that process sensitive information must have an appropriate clearance. In addition, contractors must obtain a security clearance before the Postal Service gives them access to their information and resources. While the manager of Desktop Computing was aware that appropriate security clearances were required, the Postal Service focused on the cyber intrusion remediation and did not make it a priority to validate that required clearances were in place. As a result, the Postal Service's sensitive and critical information regarding their cyber intrusion remediation efforts is at risk of exposure.

24 Handbook AS-805, Section 6-4.2.2, Information Resources Processing Sensitive-Enhanced or Sensitive Information; and ASM 14, *Administrative Support Manual*, Section 272.4, Individuals Under Service Contracts: Clearances, Roles, Background Investigations, and Denial, dated January 22, 2015.

Recommendations

We recommend management require the supplier to comply with specific security standards; complete the Certification and Accreditation process; include all appropriate provisions in their contract; modify and implement the email retention policy; assign personnel to manage access to the software; and obtain required security clearances.

We recommend the acting vice president, Information Technology, in coordination with the acting chief information security officer and Digital Solutions vice president:

1. Require the cloud service provider to move all [redacted] software – [redacted] and [redacted] information into a private cloud and become [redacted] for [redacted] – [redacted].

2. Complete the Certification and Accreditation process for the [redacted] software – [redacted] and [redacted] and obtain the physical location of Postal Service information associated with these applications.

We recommend the vice president, Supply Management:

3. Direct the contracting officer to modify the [redacted] and [redacted] software contract so that it includes Provision 4-6, System Integrity; Provision 4-7, Postal Computing Environment; and Provision 4-10, Application Information Security Requirements as required by the Supplying Principles and Practices policy.

We recommend the acting vice president, Information Technology:

4. Modify and implement Management Instruction AS 870-2011-5, *Electronic Messaging,* to require senior management emails be retained permanently and emails from other officials and contractors be retained for at least seven years; and update the Electronic Record Information System to reflect the required email retention timeframes.

5. Assign personnel to manage access to the [redacted] software and accounts in accordance with Handbook AS-805, *Information Security*, to include requesting, authorizing, terminating, and reviewing access to the software.

6. Require Postal Service employees and contractors with access to sensitive information in the [redacted] software to obtain proper security clearances and deactivate their access to the software until they obtain the proper security clearance.

Management's Comments

Management agreed with the findings and recommendations 4, 5, and 6, and the intent of recommendations 1 and 2, and disagreed with recommendation 3. Management also agreed with the monetary impact; however, they cited that the report does not provide information demonstrating that the exclusion of provisions 4-6, 4-7, and 4-10 had any actual impact on cost, schedule, or performance for the past 9 years of the contract. They also noted that Provision 4-10 was not effective until August 2008, and we should have excluded any monetary impact associated with this provision from the total.

Regarding recommendation 1, management agreed with its intent. The current [redacted] contract expires September 30, 2015, and the Postal Service issued a solicitation for a third-party provider of [redacted] on July 10, 2015. Management stated that the solicitation and resultant contract includes the required provisions and clauses for cloud security, including [redacted] certification. The target implementation date is September 30, 2015.

Regarding recommendation 2, management agreed with its intent and provided the physical location of Postal Service information associated with these applications. Management agreed to complete the C&A process for the software under the new contract. The target implementation date is December 31, 2015.

Regarding recommendation 3, management disagreed with the requirement to modify the current contract with Provisions 4-6, 4-7, and 4-10, and stated they will not modify the current contract to include these provisions. Management stated the new contract is scheduled to be in place by September 30, 2015.

Regarding recommendation 4, management agreed to update the policy to require retention of the emails of senior management and other officials as well as contractors for a period of at least 7 years per industry best practice. The target implementation date is March 31, 2016.

Regarding recommendation 5, management agreed to assign personnel to manage access to [redacted] software in accordance with Handbook AS-805, Information Security, to include requesting, authorizing, terminating, and reviewing access to the software. The target implementation date is December 31, 2015.

Regarding recommendation 6, management stated they have already taken corrective action to address the issue. The employees and contractors who are still involved in the project have obtained a clearance or are in the process of obtaining the proper clearance. The target implementation date is September 30, 2015.

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 and corrective actions should resolve the issues identified. While management disagreed with recommendation 3 to modify the current contract and include the required provisions, the OIG considers management's alternate action to include the provisions in the new contract to be responsive.

The OIG recommended modifying the [redacted] and the [redacted] software contract because the current contract has been in place since 2006. While the contract expires September 30, 2015, the Postal Service has not chosen a new supplier; therefore, [redacted] remains the current supplier. While the OIG recognizes Provision 4-10 was not effective until August 2008, the Postal Service could have issued a modification to include the provision. For instance, on October 31, 2014, the Postal Service issued Amendment of Solicitation/Modification of Contract Number 015 to include Clause 1-1, Privacy Protection, and Clause 4-19, Information Security Requirements, which were not in the original contract.

Regarding management's comments on the monetary impact, the OIG claimed this impact because the cloud service provider was not [redacted] certified for [redacted] – [redacted], and because the Postal Service did not complete the C&A process for [redacted] – [redacted] or [redacted] – [redacted] software. In addition, the Postal Service did not incorporate the required provisions in the contract. The OIG provided its monetary impact calculations to the Postal Service, which included the total [redacted] contract value of $21,980,766.41 as unsupported questioned costs for failure to comply with Postal Service policy and provisions. We also claimed $62,352 for the 3rd year of [redacted] software – [redacted] and [redacted] contract as funds put to better use.

The OIG considers recommendations 1, 2, 3, 5, and 6 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 recommendations can be closed.

Appendices

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

Appendix A: Additional Information 12
Background 12
Objectives, Scope, and Methodology 12
Prior Audit Coverage 14
Appendix B: Management's Comments ..... [redacted]

Appendix A: Additional [redacted]

Background

Cyber threats have become more sophisticated and frequent over the past decade and hackers can cause large-scale damage to institutions. The Postal Service has one of the largest networks in the world, which stores, transmits, and processes sensitive customer and employee information. To maintain the public's trust, the Postal Service must have a security system that ensures the security of its sensitive information.

In October 2014, the Postal Service became aware of a cyber intrusion that resulted in the compromise of current and former employee, customer complaints, and injury claims data. Since then management has taken action to investigate, remediate, and implement security enhancements with the goal of regaining control of the Postal Service network and preventing future attacks. During the cyber intrusion, the Postal Service determined that its exchange servers were compromised and the perpetrators could view its email communications. Therefore, the Postal Service purchased [redacted] software tenant – [redacted] to allow personnel working on remediation efforts to securely communicate with one another. They also purchased a second [redacted] software tenant – [redacted] for secure communications between Postal Service managers. The software was purchased through the Postal Service's existing contract with [redacted], a third-party vendor that provides software owned by companies such as [redacted].

The two [redacted] tenants are [redacted][25] that allows businesses to run their office automation applications and store their data using cloud computing technology. [redacted] is a set of productivity and workplace collaboration tools delivered through the cloud, which offers features such as [redacted], and email.

The Desktop Computing group administers [redacted] software, including approving and managing access to user accounts. The CISO is responsible for conducting a C&A assessment on the software and reviewing the [redacted] certification package. The Supply Management organization is responsible for managing the contract, delivery orders, and modifications for [redacted] and [redacted].

Objectives, Scope, and Methodology

Our objectives were to determine whether the Postal Service's contract for the [redacted] software complied with applicable standards, and evaluate management's adherence to the contract.

Our audit focused on the [redacted] and [redacted] software contracts. We reviewed controls over the [redacted] software tenants – [redacted] and [redacted] – but did not review a third software tenant because management did not purchase it in response to the cyber intrusion and only used it for testing purposes.

To accomplish our objectives we:

- Reviewed policies, procedures, and practices for cloud computing, electronic messaging, access, retention, contracting, and security. In addition, we reviewed best practice retention policies from the U.S. National Archives Records Administration.
- Obtained contract documentation from Supply Management personnel and the Contracting Authoring Management System and reviewed the [redacted] master contract, modifications, and delivery orders to identify clauses, conditions, and terms included in the contracts.

25 A model of service delivery where the cloud consumer controls its users and data but not the applications, platforms, or infrastructure.

- Compared the [redacted] contract and [redacted] delivery orders to the Supplying Principles and Practices to identify missing clauses and provisions.

- Interviewed Postal Service officials and [redacted] contractors to obtain documentation on the [redacted] software and cloud service, including features, level of security, and cloud service type. In addition, we interviewed management and personnel from the IT, CISO, and Supply Management offices to determine whether [redacted] and [redacted] complied with the C&A process and whether [redacted] cloud solutions were [redacted]-certified.

- Interviewed IT and the Privacy and Records Office personnel to identify email and data retention policies and processes and reviewed [redacted] software configuration settings to identify email retention periods. In addition, we interviewed IT and U.S. Postal Inspection Service personnel to identify the process for granting, terminating, and managing access to the software.

- Obtained and reviewed listings of [redacted] account users to determine the number of users for each tenant and identify any shared user accounts. In addition, we compared the listing of account users to the information listed in eAccess to identify whether users were Postal Service employees or contractors and terminated or inactive.

- Reviewed listings of inactive users to identify users who did not access their accounts within 90 days. In addition, we reviewed eAccess and interviewed Inspection Service and CISO personnel to determine whether Postal Service personnel and contractors had appropriate security clearances.

We conducted this performance audit from March through September 2015, 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on August 20, 2015, and included their comments where appropriate.

We assessed the reliability of the [redacted] user access listings and retention data by obtaining a walk-through of the data maintained in the software and interviewing Postal Service personnel and [redacted] contractors knowledgeable about the software. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
Management Alert – Overview of Information Technology Security	IT-MA-15-001	1/21/2015	None
Management of Cloud Computing Contracts and Environment	IT-AR-14-009	9/4/2014	$33,517,151
The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative	N/A	9/2014	None
Cloud Computing Contract Clauses	SM-MA-14-005	4/30/2014	$12,429,228

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

September 9, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: [redacted] Software Contract and Compliance Review (IT-AR-15-DRAFT)

Thank you for providing the Postal Service with an opportunity to review and comment on this Draft Audit Report – [redacted] Software Contract and Compliance Review. Postal Service Management notes that the [redacted] software that is the subject of this audit was purchased after the discovery that the 2014 cyber intrusion compromised Postal Service email servers. The software was used to facilitate secure communications for cybersecurity breach remediation activities. Management is in general agreement with the monetary impact and the findings and recommendations, except as noted below.

Monetary Impact:

Management agrees that solicitation Provisions 4-6 System Integrity (March 2006), Provision 4-7 Postal Computing Environment (March 2006) and Provision 4-10 Application Information Security Requirements (August 2008) were not included in the solicitation. The OIG report has identified the exclusion of these solicitation provisions from the contract as the reason for unsupported questioned costs. The report does not provide information to demonstrate that exclusion of these provisions had any actual impact on cost, schedule or performance for the past nine years of contract performance. The OIG report contends that because these provisions were not in the contract, the Postal Service was without a contractual remedy with the supplier if there was any unauthorized use, modification or disclosure of information as a result of contract performance. However, the contract incorporated Postal Service Information Technology standards and security requirements and the contract clauses and statement of work provided remedies for contractual noncompliance. The solicitation provisions alert potential offerors to the various requirements that will be in the resultant contract and the terms and conditions provide for enforcement of requirements. With the execution of the contract, the supplier acknowledged their understanding of and compliance with the requirements to abide by Postal Service software usage policies and security requirements. Additionally, the contract was awarded September 2006 and Provision 4-10 was not effective until August 2008. Therefore, any monetary impact associated with Provision 4-10 should be excluded from the total.

OIG Recommendations:

We recommend the acting vice president, Information Technology, in coordination with the acting chief information security officer and Digital Solutions vice president:

Recommendation [1]:
Require the cloud service provider to move all [redacted] software – [redacted] and [redacted] information into a private cloud and become [redacted] certified for [redacted]

Management Response/Action Plan:
Management agrees with the intent of recommendation 1; however, the current [redacted] contract expires on September 30, 2015 and a solicitation for a third party provider of [redacted] was issued on July 10, 2015. The solicitation and resultant contract includes required provisions

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

Page 1 of 4

and clauses for cloud security including [redacted] certification. Management will request closure of this recommendation once the new contract is finalized.

Target Implementation Date:
September 30, 2015

Responsible Officials:
Manager, Desktop Computing

Recommendation [2]:
Complete the Certification and Accreditation process for the [redacted] software – [redacted] and [redacted] and obtain the physical location of Postal Service information associated with these applications.

Management Response/Action Plan:
Management agrees with the intent of recommendation 2; however, the current [redacted] contract expires on September 30, 2015 and a solicitation for a third party provider of [redacted] was issued on July 10, 2015. The solicitation and resultant contract includes required provisions and clauses for cloud security. USPS management has already provided the physical location of Postal Service information associated with these applications and agrees to complete the necessary Certification and Accreditation process for software under the new contract.

Target Implementation Date:
December 31, 2015

Responsible Officials:
Manager, Corporate Information Security Office
Manager, Desktop Computing

We recommend the vice president, Supply Management:

Recommendation [3]:
Direct the contracting officer to modify the [redacted] and [redacted] software contract so that it includes Provision 4-6, System Integrity; Provision 4-7, Postal Computing Environment; and Provision 4-10, Application Information Security Requirements as required by the Supplying Principles and Practices policy.

Management Response/Action Plan:
Management disagrees with the requirement to modify the current contract with the above provisions for the following reasons:

- The current [redacted] contract expires on September 30, 2015. A solicitation for [redacted] was issued on July 10 and the solicitation included Provision 4-6, System Integrity; Provision 4-7, Postal Computing Environment; and Provision 4-10, Information Security Requirements.
- We would not modify a contract to include Provisions; these are applicable during the solicitation phase when establishing a contract. Once the contract is awarded, any additional clauses or requirements would require a modification. Provision 4-10 was issued two years after contract formation and would not have been available at the time of solicitation. Additionally, Cloud policies and [redacted] certification requirements were not in effect at the time the contract was solicited and established.
- Though the above cited provisions were not within the 2006 solicitation, the solicitation and resultant contract have a statement of work and clauses that incorporate Postal Service Information Technology standards and security requirements that were in use at the time of contract award. The supplier acknowledged with their proposal and signing of

the contract, their understanding of, and agreement with Postal Service requirements for software usage and security.

Target Implementation Date:
N/A

Responsible Officials:
Manager, Technology Infrastructure Portfolio, Supply Management

We recommend the acting vice president, Information Technology:

Recommendation [4]:
Modify and implement Management Instruction AS 870-2011-5, Electronic Messaging, to require senior management emails be retained permanently and emails from other officials and contractors be retained for at least seven years; and update the Electronic Record Information System to reflect the required email retention timeframes.

Management Response/Action Plan:
Management agrees in part with the recommendation and will update policy to require that senior management and other emails be retained for a period of at least 7 years per industry best practice.

Target Implementation Date:
March 31, 2016

Responsible Officials:
Manager, Desktop Computing

Recommendation [5]:
Assign personnel to manage access to the [redacted] software and accounts in accordance with Handbook AS-805, Information Security, to include requesting, authorizing, terminating, and reviewing access to the software.

Management Response/Action Plan:
Management agrees with the recommendation and will assign personnel to manage access to the [redacted] software in accordance with Handbook AS-805, Information Security, to include requesting, authorizing, terminating, and reviewing access to the software.

Target Implementation Date:
December 31, 2015

Responsible Officials:
Manager, Desktop Computing

Recommendation [6]:
Require Postal Service employees and contractors with access to sensitive information in the [redacted] software to obtain proper security clearances and deactivate their access to the software until they obtain the proper security clearance.

Management Response/Action Plan:
Management agrees with the recommendation and has already taken corrective action to address the issue. The manager, Desktop Computing has validated the list of Postal Service employees and contractors who did not have proper clearance and noted that many people are no longer involved with the project. Those that are remaining for support either have clearances or are in the process of obtaining the proper clearance. Management will request that this recommendation be closed once evidence of the clearances is provided.

475 L'Enfant Plaza SW
Washington, DC 20260-5000
www.usps.com

Target Implementation Date:
September 30, 2015

Responsible Official:
Manager, Desktop Computing

Judith A. Adams
(A) Vice President, Information Technology

Gregory S. Crabb
(A) Chief Information Security Officer and Digital Solutions Vice President

Susan M. Brownell
Vice President, Supply Management

cc: *Corporate Audit Response Management*

475 L'Enfant Plaza SW
Washington, DC 20260-5000
www.usps.com

Page 4 of 4

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

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