U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

AUDIT REPORT
REPORT NUMBER 16-22

Cloud Computing: Transition of GPO's Integrated Library System

September 30, 2016

GPO U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

September 30, 2016

To

Chief Information Officer
Chief, Acquisition Services

From

Inspector General

Subject:

Audit Report—Cloud Computing: Transition of GPO's Integrated Library System
Report Number 16-22

Enclosed please find the subject final report. Please refer to the "Results in Brief" for the overall audit results. Our evaluation of your response has been incorporated into the body of the report. We consider management's comments responsive to the three recommendations, which are considered resolved but will remain open until implementation of the proposed corrective actions.

We appreciate the courtesies extended to the staff during our audit. If you have any questions or comments about this report, please do not hesitate to contact Mr. Phillip M. Faller, Assistant Inspector General for Audits and Inspections at (202) 512-2009 or me at (202) 512-0039.

Michael A Raponi
MICHAEL A. RAPONI
Inspector General

Attachment

cc:
Director, GPO
Deputy Director, GPO
General Counsel
Chief of Staff
Chief Administrative Officer

Contents

Office of Inspector General

Report Number 16-22 **September 30, 2016**

Cloud Computing: Transition of GPO's Integrated Library System

Introduction

Since 2006, GPO has used a commercial-off-the-shelf Integrated Library System (ILS) software product called ALEPH®. Ex Libris Group, Inc. developed the software. ILS supports two statutorily mandated programs—the Federal Depository Library Program and the Cataloging and Indexing Program. Also since 2006, Progressive Technology Federal Systems (PTFS), a GPO contractor, has provided software maintenance service and hosted hardware capable of sustaining both programs at its data center located in Sterling, Virginia.

In April 2015, GPO awarded PFTS its second contract to continue providing support services. In September 2015, GPO exercised a 1-year option to extend support services through September 2016. In May 2015, however, PTFS notified GPO it intended to transition ILS from the data center in Sterling to the Amazon Web Service—a cloud computing service provider. PTFS reported the transition was completed in January 2016. The award amount, which spanned from April 1, 2015, through September 30, 2016, totaled $681,022.

The Office of Inspector General (OIG) conducted an audit to determine the steps GPO took when it transitioned the ILS administered by PFTS to Amazon Web Services. To accomplish the objective, we reviewed contract and technical records pertaining to the transition, applicable GPO policies and procedures, and Federal cloud computing guidance as well as interviewed officials with oversight responsibility. We conducted this performance audit from April through September 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the results of the audit provide a reasonable basis for our findings and conclusions based on our objective. See Appendix A for details of our objectives, scope, methodology, and criteria.

Results in Brief

Transitioning to a hosted service was in response to the Office of Management and Budget (OMB) Federal Cloud First guidance. According to officials, the transition occurred without disruption to the Federal Depository Library Program or the

Cataloging and Indexing Program. Although no reportable disruptions occurred, the following areas require management attention:

- GPO policy did not include Cloud Computing and/or Hosted Service definitions, principles, rules, and guidelines.

- Personnel did not follow Configuration Management policy during transition to the Amazon Web Services.

- Contract language did not address hosted services.

Without established policies and definitive processes for transitioning information technology (IT) investment to a hosted service, management could not ensure a consistency of comparing costs and benefits across various transition projects, that transition projects were monitored and provided with adequate management oversight, or that completed transition projects were consistently evaluated to determine overall organizational performance improvement.

Although the Amazon Web Services is authorized by Federal Risk and Authorization Management Program (FedRAMP),[1] lack of appropriate contract language for data ownership established an increased risk. Such a risk could have allowed the cloud provider with unnecessary access to Federal data. In addition, failure to define security standards and testing requirements increased the risk of a data breach, which could have led to the loss or corruption of data.

Recommendations

1. We recommend the Chief Information Officer develop a policy that defines and implements key principle actions pertaining to "cloud computing" and "hosted services."

2. We recommend the Chief, Acquisition Services revise the contract to include cloud computing in accordance with best practices as the Chief Information Officers Council and Chief Acquisition Officers Council define.

Management's Response and Our Evaluation

Management concurred with the recommendations. We consider the recommendations resolved but will remain open until implementation of the corrective actions. The complete text of management's response is in Appendix C.

[1] As of May 2013, the Amazon Web Services met FedRAMP requirements.

Background

Cloud computing enables convenient, on-demand access to shared computing resources that can be rapidly provided to users. In February 2011, OMB issued the Federal Cloud Computing Strategy.[2] The strategy provides definitions of cloud computing services; benefits of cloud services, such as accelerating data center consolidations; a decision framework for migrating services to a cloud environment; case studies to support agency migration to cloud computing services; and roles and responsibilities for Federal agencies. As part of this strategy, OMB instituted a "Cloud First" policy designed to accelerate the pace with which cloud computing technologies are adopted and used by the Federal Government.

In March 2006, GPO released the Integrated Library System (ILS) to enhance its online computer environment in support of two statutorily mandated programs:

- Federal Depository Library Program—GPO disseminates information products from the three branches of the Federal Government to Federal depository libraries nationwide. The program provides free online access to Government publications via GPO's Federal Digital System (FDsys).

- Cataloging and Indexing Program—GPO creates cataloging and a comprehensive index for public documents issued or published by the Federal Government that are not confidential in nature.

In May 2015, PTFS notified GPO they intended to transition ILS from its data center located in Sterling, Virginia to the Amazon Web Service—an approved FedRAMP[3] cloud computing service provider. On December 31, 2015, PTFS reported it successfully transitioned the following ILS-related Web sites to the Amazon Web Services:

- The Catalog of U.S. Government Publications – http://catalog.gpo.gov;

- The Federal Depository Library Directory – http://catalog.gpo.gov/fdlpdir/FDLPdir.jsp; and

- MetaLib – http://metalib.gpo.gov/.

On January 1, 2016, PTFS reported the transition was complete and the public could access ILS through the Amazon Web Services.

[2] OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: February 8, 2011).

[3] OMB established FedRAMP, a Government-wide program intended to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud computing products and services. All Federal agencies must meet FedRAMP requirements when using cloud services, and the cloud service providers must implement the FedRAMP security requirements in their cloud environment.

Responsibilities

The Chief Information Officer is responsible for Configuration Management governance at GPO.[4] The Chief, Acquisition Services (Chief Acquisition Officer) is responsible for ensuring that contracts are made in accordance with applicable laws, regulations, and directives. [5] The Superintendent of Documents is responsible for the Federal Depository Library Program and the Cataloging and Indexing Program.

[4] GPO Directive 825.8, *Information Technology Configuration Management Policy*, dated November 22, 2013.

[5] GPO Instruction 110.5D, *Acquisition Authority, Policies, and Responsibilities*, dated March 19, 2004.

Results and Recommendations

GPO's transition to a hosted service was in response to the OMB Federal Cloud First guidance. Although no reportable disruptions were noted, the following areas require management attention.

- GPO policy did not include Cloud Computing and/or Hosted Service definitions, principles, rules, and guidelines.

- Personnel did not follow Configuration Management policy during transition to the Amazon Web Services.

- Contract language did not address hosted services.

<u>Policy Did Not Include Cloud Computing and/or Hosted Service Framework</u>

GPO did not have an established framework for developing, approving, implementing, reviewing, and maintaining cloud computing services.

Policy[6] requires that management controls provide reasonable assurance and safeguards for protecting assets against waste, loss, unauthorized use, and misappropriation. It also requires that GPO maintain effective systems of accounting and management control. The policy states that internal controls are the organization, policies, and procedures used to reasonably ensure that:

- Programs achieve intended results.
- Resources are used consistent with agency mission.
- Programs and resources are protected from waste, fraud, and mismanagement.
- Laws and regulations are followed.
- Reliable and timely information is obtained, maintained, reported, and used for decision making.

The Government Accountability Office *Standards for Internal Controls in the Federal Government*, September 2014, require that management clearly document internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records must be properly managed and maintained.

[6] GPO Instruction 825.18A, *Internal Control Program*, dated May 28, 1997.

Configuration Management Policy Not Followed

GPO Directive 825.8, *Information Technology Configuration Management Policy,* dated November 22, 2013, establishes a policy for controlling changes within the GPO IT plans, infrastructures, applications, services, and standards. The policy requires that any approved changes to GPO-wide IT plans, policies, infrastructure components, operating systems, networking software, security software, projects, applications, systems, IT products, licenses, associated configurations, and released deliverables are documented under Configuration Management governance.

A comparison of GPO's Configuration Management Policy to activities associated with transitioning ILS to the Amazon Web Services revealed inconsistencies. The following requirements were not met.

- *Configuration Management Plan Not Developed*. Management did not develop or maintain an updated Configuration Plan. GPO policy states that the Configuration Management Plan must be the master plan used for providing GPO with configuration controls for any approved configurable items within IT products and projects. Configuration Management serves as the controlling discipline for preserving product and system integrity. The plan highlights the roles and responsibilities of areas involved in the Configuration Management activity for a project.

- *ILS Not Incorporated within the Configuration Management Database.* Management did not incorporate ILS within the Configuration Management Database. GPO policy requires that project phases and gates documentation and associated approvals are submitted and incorporated as a system of records within the Configuration Management Database. Review of the System Security Plan, Security Authorization, and Sequencing Plan revealed that no documentation existed that was associated with project phases and gates necessary to incorporate in the Configuration Management Database. The Configuration Management Database is a required document under the System Development Life Cycle, Phase 3, Functional Requirement.[7] Officials stated that they did not prepare this database.

- *Hosted Service Not Included in the Baseline or Target Architecture.* Although it documented the ILS in the Architecture, management did not document it as a hosted service.

[7] GPO Directive 705.28, *GPO Information Technology System Development Life Cycle Policy,* dated December 12, 2005.

Absence of Contract Language Reflecting Hosted Services

The appropriate contract language as Federal guidance defines for hosted services provided by the Amazon Web Services was missing.

In February 2012, the CIO Council and Chief Acquisition Officers Council published a document entitled, "Chief Information Officers Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government*, *Best Practices for Acquiring IT as a Service."* The document establishes best practices for acquiring IT as a service and suggests addressing the following areas when creating a cloud computing contract.

- *Selecting a Cloud Service.* Choosing the appropriate cloud service and deployment model is the critical first step in procuring cloud services.

- *Cloud Service Providers and End-User Agreements.* Terms of Service and all Cloud Service Provider/customer-required agreements should be integrated fully into cloud contracts.

- *Service Level Agreements.* Service Level Agreements (SLAs) should define performance with clear terms and definitions, demonstrate how performance will be measured, and the enforcement mechanisms in place for ensuring SLAs are met.

- *Cloud Service Provider, Agency, and Integrator Roles and Responsibilities.* Careful delineation between the responsibilities and relationships among the Federal agency, integrators, and the Cloud Service Provider are needed in order to effectively manage cloud services.

- *Standards.* Use of the National Institute of Standards and Technology (NIST) cloud reference architecture as well as agency involvement in standards are necessary for cloud procurements.

- *Security.* Agencies must clearly detail the requirements for Cloud Service Providers to maintain the security and integrity of data existing in a cloud environment.

- *Privacy.* If cloud services host "privacy data," agencies must adequately identify potential privacy risks and responsibilities and address these needs in the contract.

- *E-Discovery.* Federal agencies must ensure that data stored in a Cloud Service Provider environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced.

- *Freedom of Information Act.* Federal agencies must ensure that any data stored in a Cloud Service Provider environment is available for appropriate handling under the Freedom of Information Act *(*FOIA).

- *E-Records.* Agencies must ensure Cloud Service Provider's understand and assist Federal agencies in compliance with the Federal Records Act of 1950 and obligations under that law.

According to Subpart 4.801(b) of GPO Publication 805.33, *Materials Management Acquisition Regulation (MMAR)*, dated May 15, 2003, documentation in files must be sufficient to constitute a complete history of the transactions for the purpose of: (1) providing a complete background as a basis for informed decisions at each step of the acquisition process; (2) supporting actions taken; (3) providing information for reviews and investigations; and (4) furnishing essential facts in the event of litigation or congressional inquiries.

Acquisition Services stated that neither a contract nor contract modification was executed. Officials could not provide a reason for the lack of contract execution.

Recommendations

1. We recommend the Chief Information Officer develop a policy that defines and implements key principle actions pertaining to "cloud computing" and "hosted services."

Management's Response

Management concurred with the recommendation.

Evaluation of Management's Response

Management's proposed corrective actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending implementation of the planned actions.

2. We recommend the Chief, Acquisition Services revise the contract to include language requiring that cloud computing is in accordance with best practices as defined by the Chief Information Officers Council and Chief Acquisition Officers Council.

Management's Response

Management concurred with this recommendation.

Evaluation of Management’s Response

Management’s proposed corrective actions are responsive to the recommendation. The recommendation is resolved but will remain open for reporting purposes pending implementation of the planned actions.

Appendix A – Objective, Scope, and Methodology

We performed fieldwork from April through September 2016 in Washington, D.C., in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides 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 objective.

Objective

The objective of our audit was to review the steps GPO took when it transitioned its ILS—administered by PFTS to the Amazon Web Services.

Scope and Methodology

To accomplish our objective, we—

- Reviewed contract and technical records pertaining to the transition.
- Reviewed applicable GPO policies and procedures as well as Federal cloud computing guidance.
- Interviewed officials with oversight responsibility.

Management Controls Reviewed

We determined that the following internal controls were relevant to our audit objective:

Program Operations – Policies and procedures GPO management implemented to reasonably ensure contracts are properly awarded.

Compliance with Laws and Regulations – Policies and procedures that management implemented to reasonably ensure that resource use is consistent with laws and regulations.

The details of our examination of management controls, the results of our examination, and noted management control deficiencies are contained in the report narrative. Implementing the recommendations in this report should improve those management control deficiencies.

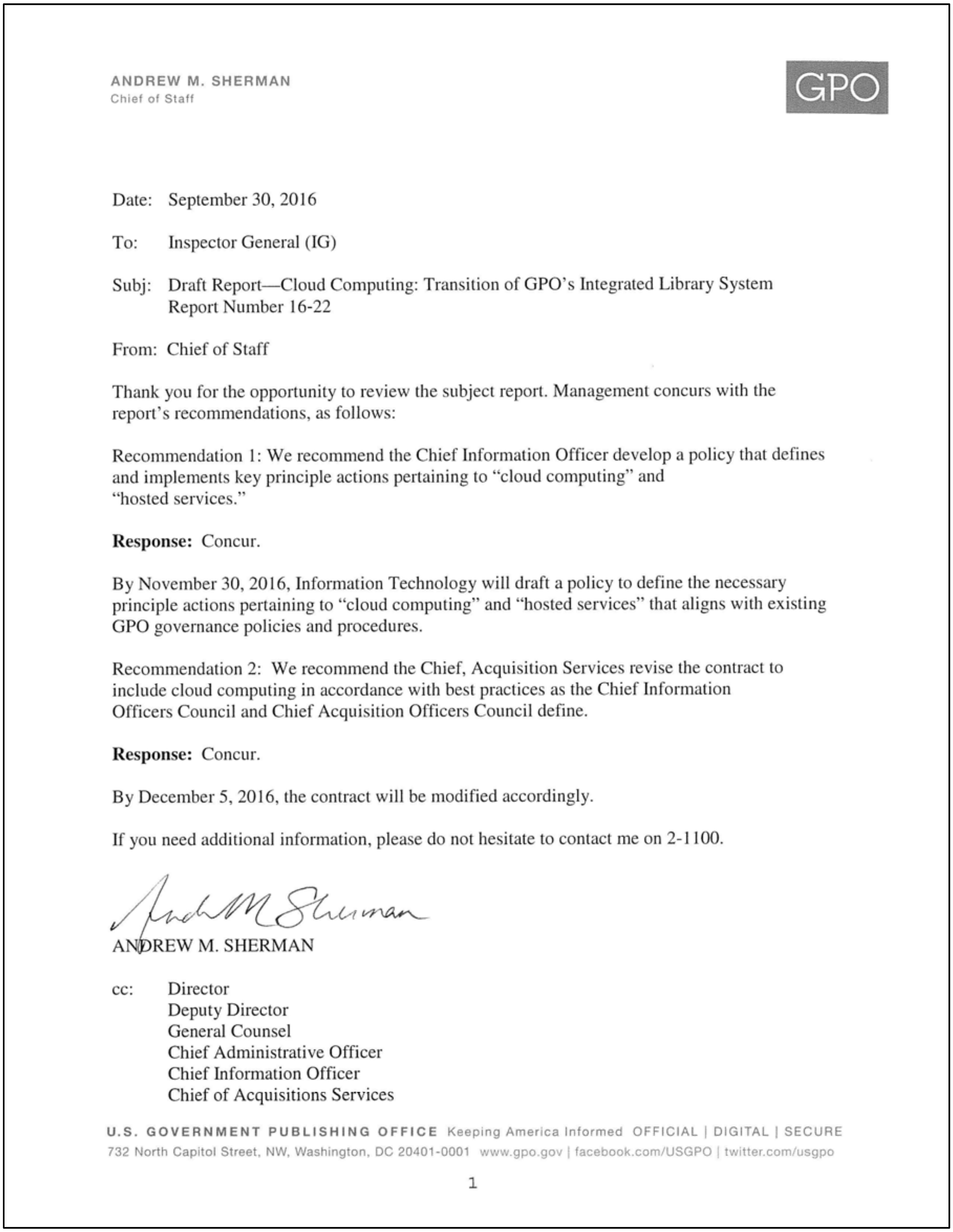
Computer-Generated Data

We did not use computer-processed information for this audit.

Appendix B – Acronyms and Abbreviations

CIO	Chief Information Officer
FDsys	Federal Digital System
FedRAMP	Federal Risk and Authorization Management Program
FOIA	Freedom of Information Act
GPO	Government Publishing Office
ILS	Integrated Library System
IT	Information Technology
MMAR	Materials Management Acquisition Regulation
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PTFS	Progressive Technology Federal Systems
SLA	Service Level Agreements

Appendix C – Management's Response



ANDREW M. SHERMAN
Chief of Staff

GPO

Date: September 30, 2016

To: Inspector General (IG)

Subj: Draft Report—Cloud Computing: Transition of GPO's Integrated Library System
Report Number 16-22

From: Chief of Staff

Thank you for the opportunity to review the subject report. Management concurs with the report's recommendations, as follows:

Recommendation 1: We recommend the Chief Information Officer develop a policy that defines and implements key principle actions pertaining to "cloud computing" and "hosted services."

Response: Concur.

By November 30, 2016, Information Technology will draft a policy to define the necessary principle actions pertaining to "cloud computing" and "hosted services" that aligns with existing GPO governance policies and procedures.

Recommendation 2: We recommend the Chief, Acquisition Services revise the contract to include cloud computing in accordance with best practices as the Chief Information Officers Council and Chief Acquisition Officers Council define.

Response: Concur.

By December 5, 2016, the contract will be modified accordingly.

If you need additional information, please do not hesitate to contact me on 2-1100.

Andrew M Sherman
ANDREW M. SHERMAN

cc: Director
Deputy Director
General Counsel
Chief Administrative Officer
Chief Information Officer
Chief of Acquisitions Services

Appendix D - Status of Recommendations

Recommendation	Resolved	Unresolved	Open/ECD*	Closed
1	X		November 30, 2016	
2	X		December 5, 2016	

*Estimated Completion Date.

Appendix E – Report Distribution

Director, GPO
Deputy Director, GPO
General Counsel
Chief of Staff
Chief Administrative Officer

Major Contributor to the Report

Tony Temsupasiri – Lead Information Technology Specialist