



OFFICE OF INSPECTOR GENERAL

Audit Report

2014-IT-C-016

Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services

September 30, 2014

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Khalid Hasan, OIG Manager

Paul Vaclavik, Auditor in Charge

Joshua Dieckert, IT Auditor

Peter Sheridan, Senior OIG Manager

Andrew Patchan Jr., Associate Inspector General for Information Technology

Abbreviations

AWS	Amazon Web Services
CAT	Compliance Analysis Toolkit
CFPB	Consumer Financial Protection Bureau
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSP	cloud service provider
e-discovery	electronic discovery
FAR	<i>Federal Acquisition Regulation</i>
IaaS	infrastructure as a service
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PaaS	platform as a service
SaaS	software as a service
SLA	service-level agreement
Treasury	U.S. Department of the Treasury



Executive Summary:

Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services

2014-IT-C-016

September 30, 2014

Purpose

In January 2014, the Council of the Inspectors General on Integrity and Efficiency initiated a government-wide review of select agencies' efforts to adopt cloud computing technologies. In support of this initiative, our objective was to review the Consumer Financial Protection Bureau's (CFPB) acquisition and contract management for Amazon.com's Amazon Web Services and Deloitte's Compliance Analysis Toolkit to determine whether requirements for security, service levels, and access to records were planned for, defined in contracts, and being monitored.

Background

Cloud computing refers to a model for delivery of information technology (IT) services through on-demand access to a pool of configurable computing resources. Federal agencies, including the CFPB, are increasingly adopting cloud computing to lower IT costs and gain efficiencies.

The CFPB's strategic plan emphasizes the need for a flexible, scalable IT infrastructure that is capable of meeting current needs and sustaining the agency's future growth. To help achieve this objective, the CFPB has contracted with seven cloud service providers (CSPs), including Amazon.com, which hosts the agency's public website, and Deloitte, which provides an application that allows financial companies that are supervised by the CFPB to upload loan file data for analysis by the agency's examiners.

Findings

Overall, we found that the CFPB's contracts for cloud computing services with Amazon.com and Deloitte included roles and responsibilities, information security requirements, and service-level expectations. We also found that the CFPB has established a process to monitor both contractual and service-level requirements for its CSPs, and that the agency collects and maintains nondisclosure agreements from contractor personnel to protect sensitive information.

We identified opportunities for improvement in the procurement and use of cloud services. Specifically, we found that when the CFPB began operations in July 2011, it used a U.S. Department of the Treasury contract with Amazon.com to quickly meet its IT needs. The agency, however, did not perform its own alternatives and cost analysis at that time. In addition, we found that the CFPB's cloud computing contracts and service-level agreements with both Amazon.com and Deloitte did not include clauses providing the access needed for electronic discovery and performance of criminal and noncriminal investigations. We also found that the CFPB's contract with Deloitte did not include a clause granting the Office of Inspector General the right to examine agency records or detail specific penalties or remedies for noncompliance with contract terms and service levels.

Recommendations

Our report contains four recommendations to assist the CFPB's Chief Information Officer in strengthening processes for the acquisition and contract management of cloud services. Specifically, we recommend that the Chief Information Officer ensure that alternatives and cost analyses are conducted, assess the costs and benefits of negotiating post-award agreements with Amazon.com and Deloitte to include relevant requirements and best practices, ensure that agency guidance used to develop contracts and service-level agreements with CSPs references applicable *Federal Acquisition Regulation* and best practice contract clauses, and ensure that future CFPB contracts for cloud computing services include relevant requirements and best practice contract clauses. The Chief Information Officer concurred with our recommendations and outlined actions that have been taken or will be implemented to address our recommendations.

Access the full report: <http://oig.consumerfinance.gov/reports/cfpb-cloud-computing-services-sep2014.htm>

For more information, contact the OIG at 202-973-5000 or visit <http://oig.consumerfinance.gov>.

Summary of Recommendations, OIG Report No. 2014-IT-C-016

Rec. no.	Report page no.	Recommendation	Responsible office
1	5	Ensure that an alternatives and cost analysis is conducted to inform the selection of cloud computing service providers and models.	Office of the Chief Information Officer
2	7	Assess the costs and benefits of negotiating post-award agreements with Amazon.com and Deloitte to include clauses for Inspector General information access, the conduct of forensic investigations and electronic discovery, and penalties for noncompliance with contract and service-level agreement terms, as appropriate.	Office of the Chief Information Officer
3	7	Ensure that the guidance used to develop contracts and service-level agreements with cloud service providers references <i>Federal Acquisition Regulation</i> requirements and best practice contract clauses for information access, conduct of forensic investigations and electronic discovery, and penalties for noncompliance, as appropriate.	Office of the Chief Information Officer
4	7	Ensure that future CFPB contracts for cloud computing services include <i>Federal Acquisition Regulation</i> requirements and best practice clauses for information access, the conduct of forensic investigations and electronic discovery, and the assessment of penalties for noncompliance with contract and service-level agreement terms.	Office of the Chief Information Officer



OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

September 30, 2014

MEMORANDUM

TO: Ashwin Vasani
Chief Information Officer
Consumer Financial Protection Bureau

FROM: Andrew Patchan Jr. *Andrew Patchan Jr.*
Associate Inspector General for Information Technology

SUBJECT: OIG Report No. 2014-IT-C-016: *Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services*

The Office of Inspector General (OIG) has completed its report on the subject audit. In January 2014, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) initiated a government-wide review of select agencies' efforts to adopt cloud computing technologies. The CIGIE initiative focused on reviewing cloud computing contracts for inclusion of specific clauses and the agencies' efforts to monitor the performance of cloud service providers. In support of the CIGIE initiative, our objective was to review the Consumer Financial Protection Bureau's (CFPB) acquisition and contract management for Amazon.com's Amazon Web Services and Deloitte's Compliance Analysis Toolkit to determine whether requirements for security, service levels, and access to records were appropriately planned for, defined in contracts, and being monitored. We provided CIGIE with responses to a questionnaire it issued to the select agencies' OIGs under a separate cover. This report includes specific findings and recommendations designed to assist the CFPB in improving its acquisition and contract management processes associated with cloud service providers.

We provided a draft of our report to you for review and comment. In your response, included as appendix B, you concurred with our recommendations and outlined actions that have been taken, are underway, and are planned to address our recommendations.

We appreciate the cooperation that we received from CFPB personnel during our review. Please contact me if you would like to discuss this report or any related issues.

cc: Sartaj Alag, Chief Operating Officer
Stephen Agostini, Chief Financial Officer
Zachary Brown, Chief Information Security Officer
J. Anthony Ogden, Deputy Inspector General
Matthew Simber, OIG Manager for Policy, Planning, and Quality Assurance

Contents

Introduction	1
Objectives	1
Background	1
Federal Guidance and Best Practices for Acquiring Cloud Computing Services	2
Finding 1: The CFPB’s Business Case for AWS Did Not Include an Alternatives and Cost Analysis	4
Recommendation	5
Management’s Response	5
OIG Comment	5
Finding 2: Specific Clauses for Information Access and Penalties for Noncompliance Were Not Included in CSP Contracts and SLAs	6
Recommendations	7
Management’s Response	8
OIG Comment	8
Appendix A: Scope and Methodology	9
Appendix B: Management’s Response	10

Introduction

Objectives

In January 2014, the Council of the Inspectors General on Integrity and Efficiency (CIGIE)¹ initiated a government-wide review of select agencies' efforts to adopt cloud computing technologies. The initiative focused on reviewing cloud computing contracts for inclusion of specific clauses and the agencies' efforts to monitor the performance of cloud service providers (CSPs). In support of the CIGIE initiative, our objective was to review the Consumer Financial Protection Bureau's (CFPB) acquisition and contract management for Amazon.com's Amazon Web Services (AWS) and Deloitte's Compliance Analysis Toolkit (CAT) to determine whether requirements for security, service levels, and access to records were appropriately planned for, defined in contracts, and being monitored. We provided CIGIE with responses to a questionnaire it issued to the select agencies' OIGs under a separate cover. Appendix A provides our scope and methodology.

Background

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST classifies cloud computing capabilities into the following three models:

1. Software as a service (SaaS) provides the capability to use the CSP's applications running on a cloud infrastructure.
2. Platform as a service (PaaS) refers to the capability to deploy consumer-created or -acquired applications that are developed using programming languages and tools supported by the CSP onto the cloud infrastructure.
3. Infrastructure as a service (IaaS) enables provisioning of processing, storage, networks, and other computing resources where the consumer is able to deploy, run, and control software applications.²

Cloud computing offers federal agencies the potential for cost savings through faster deployment of computing resources, a decreased need to buy hardware or build data centers, and enhanced collaboration capabilities. Recognizing these benefits, the Office of Management and Budget issued a *Cloud First* policy in December 2010, requiring federal agencies to evaluate safe, secure cloud computing options before making new investments in information technology (IT).

-
1. CIGIE was statutorily established as an independent entity within the executive branch by the Inspector General Reform Act of 2008, P.L. 110-409, to address integrity, economy, and effectiveness issues that transcend individual government agencies.
 2. National Institute of Standards and Technology, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, May 2012.

When it began operations in July 2011, the CFPB relied on the U.S. Department of the Treasury (Treasury) for IT systems and services. As the agency transitions IT systems and services from Treasury, it has increasingly embraced cloud computing as a model to meet its IT needs in a flexible, scalable manner. Specifically, the CFPB has contracted with seven CSPs, including Amazon.com and Deloitte. Amazon.com hosts the CFPB’s public website and provides infrastructure for the agency’s software development efforts through AWS. Deloitte provides the agency’s CAT, which is an application that allows financial companies that are supervised by the CFPB to upload loan file data for analysis by the agency’s examiners. As highlighted in table 1, the CFPB also uses cloud computing solutions for automated litigation support and for contact center services. As of June 2014, the CFPB’s cloud computing contracts were valued at approximately \$185 million.

Table 1: Summary of Cloud Computing Technologies Used by the CFPB

CSP	Cloud service description	Type of cloud service	Total contract value	Contract initiation date	Contract length
General Dynamics	Contact center support and services	SaaS	\$131,000,000	06/08/2011	5 years
Deloitte	CAT, analytical services, and support	SaaS	\$25,000,000	05/29/2012	5 years
Treasury	IT shared services	PaaS	\$9,674,580	10/01/2013	1 year
Treasury	Financial management services	PaaS	\$7,075,604	10/01/2013	1 year
Verizon Terremark	Data storage/colocation	IaaS	\$4,200,000	01/05/2011 ^a	8 months
Amazon.com	Web hosting	IaaS	\$4,200,000	01/05/2011 ^a	8 months
U.S. Department of Justice	Automated litigation support	SaaS	\$3,997,840	05/12/2012	5 years

Source: Information taken from the CFPB’s responses to the CIGIE cloud computing survey.

^aThe CFPB initially contracted with Verizon Terremark and Amazon.com for cloud services on January 5, 2011. The contract values and lengths reflected in the table are for the most recent contract extensions the CFPB signed with these two companies on January 1, 2014.

Federal Guidance and Best Practices for Acquiring Cloud Computing Services

Compared to traditional IT contracts, procuring cloud computing services presents agencies with unique and differing risks to manage. For instance, CSPs may store data across multiple facilities across the world. Thus, federal agencies must carefully consider who may have access to data and under what circumstances. To ensure that federal agencies are procuring cloud services in accordance with existing regulations and laws, the Chief Information Officers Council and the Chief Acquisition Officers Council issued guidance on February 24, 2012, for creating effective

cloud computing contracts for the federal government.³ This guidance highlights the importance of clearly defining in contracts roles and responsibilities between the CSP and the agency, particularly with respect to information access. The guidance also recommends that agencies establish service-level expectations and monitor CSP compliance, ensure control of federal data through completion of nondisclosure agreements, and include clauses in contracts or agreements outlining procedures for conducting forensic investigations and electronic discovery (e-discovery).

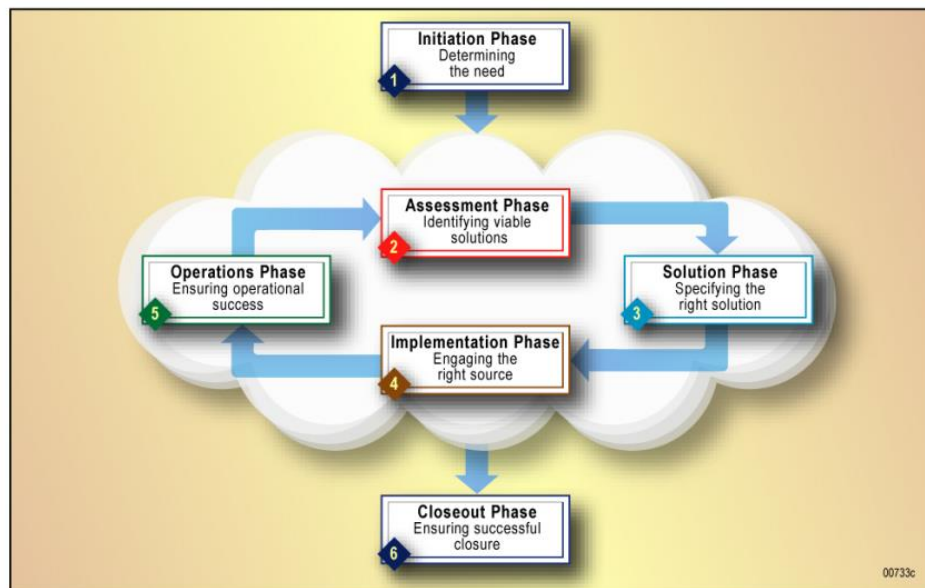
Guidance issued by NIST on cloud computing and procurement of IT services also provides best practices that agencies may consider when acquiring cloud services. For instance, NIST Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012, notes that an agency should develop a business case for moving to the cloud that considers the readiness of existing applications for cloud deployment, transition and life cycle costs, and security and privacy requirements. Further, NIST Special Publication 800-35, *Guide to Information Technology Security Services*, October 2002, presents factors for agencies to consider when selecting, implementing, and managing IT security services and providers. These factors can also apply to the procurement of cloud services and include consideration of viable alternatives, development of cost estimates, and formalization of service-level agreements (SLAs) with specific clauses and terms unique to each organization.

³ The Chief Information Officers Council was established in July 1996 by Executive Order 13011, *Federal Information Technology*, with the mission to improve practices related to the design, acquisition, development, use, sharing, and performance of federal government information resources. The Chief Acquisition Officers Council was established in 1999, pursuant to section 16 of the Office of Federal Procurement Policy Act, and it seeks to promote effective business practices that ensure the timely delivery of products and services to agencies, achieve public policy objectives, and further openness in the federal acquisition system.

Finding 1: The CFPB's Business Case for AWS Did Not Include an Alternatives and Cost Analysis

As part of planning to acquire cloud services, NIST Special Publication 800-146 states that agencies should develop a business case that considers the readiness of existing applications for cloud deployment, transition and life cycle costs, and security and privacy requirements. In addition, NIST Special Publication 800-35 details an IT security services life cycle that provides a framework for use in selecting, implementing, and managing IT security services, including cloud computing services. Figure 1 details NIST's IT security services life cycle. The solution phase involves the development of a business case in order to identify the best solution to produce the desired future state. Specifically, the business case should include consideration of viable alternatives, formation of cost estimates, and completion of an organizational risk analysis. In accordance with this life cycle approach, the CFPB is in the process of strengthening its IT capital planning program to guide the selection, evaluation, and control of its IT investments. As part of this program, the CFPB has created an Investment Review Board designed to review the agency's business cases for IT investment decisions.

Figure 1: IT Security Services Life Cycle



Source: NIST SP 800-35, *Guide to Information Technology Security Services*

We found that although a business case analysis was completed to guide the CFPB's acquisition of CAT, the alternatives and cost savings analysis part of the business case analysis for the AWS cloud computing environment was not completed. An alternatives and cost savings analysis was not completed for the AWS contract because the CFPB's current investment review process was not in place when that contract was initially awarded. In addition, CFPB officials informed us that at the time the AWS contract was awarded, the agency had recently been established as an

independent agency and it had to rapidly establish its IT infrastructure to support its needs. As such, the agency utilized an existing Treasury contract with Amazon.com without performing its own alternatives and cost savings analysis.

The Chief Information Officer stated that as the CFPB continues to transition its IT infrastructure from Treasury, the agency will be evaluating various models, including cloud computing and in-house approaches, to hosting its infrastructure. Completion of a business case for proposed approaches that includes viable alternatives and cost considerations will provide key information to assist CFPB officials in selecting an IT infrastructure solution that best meets the needs of the agency in a cost-effective manner.

Recommendation

We recommend that the Chief Information Officer

1. Ensure that an alternatives and cost analysis is conducted to inform the selection of cloud computing service providers and models.

Management's Response

The Chief Information Officer concurs with this recommendation and is working to continue to mature the agency's processes, to include conducting the appropriate reviews during source selection as well as cost-benefit and trade-off analyses.

OIG Comment

In our opinion, the actions described by the Chief Information Officer are responsive to our recommendation. We plan to follow up on the actions to ensure that the recommendation is fully addressed.

Finding 2: Specific Clauses for Information Access and Penalties for Noncompliance Were Not Included in CSP Contracts and SLAs

As shown in figure 1 above, once a business case has been reviewed and a service provider has been selected as part of the solution phase, the implementation phase begins. This phase includes the development of an SLA with specific clauses and terms unique to each organization. *Federal Acquisition Regulation (FAR) section 52.215-2, Audit and Records*, requires that contracts for cloud computing include a clause related to granting the OIG access and the right to examine any of the directly pertinent records involving transactions related to the contract. Further, best practices for creating effective cloud computing contracts in the federal government stipulate that penalties for noncompliance with contract and service agreement terms, as well as procedures for e-discovery and forensic investigations, should be outlined in the contract or the SLA between the agency and the CSP.⁴

We found that the CFPB's contracts for cloud computing services with Amazon.com and Deloitte included specific clauses covering roles and responsibilities, information security requirements, and service-level expectations. We also found that the CFPB has established a process to monitor both contractual and service-level requirements for its CSPs and that the agency collects and maintains nondisclosure agreements from contractor personnel to protect sensitive information. However, as highlighted in table 2, we identified that the contracts and SLAs for both AWS and CAT did not include clauses covering (1) the conduct of forensic investigations for criminal and noncriminal purposes and (2) procedures for e-discovery when conducting a criminal investigation. Additionally, we found that the CAT contract did not include FAR clause 52.215-2 related to granting the OIG access to contractor records or include clauses specifying penalties levied on the CSP for noncompliance with contract or SLAs.

4. See CIO Council and Chief Acquisition Officers Council, in coordination with the Federal Cloud Compliance Committee, *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*, February 24, 2012, <https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf>.

Table 2: Select Best Practice Contract and SLA Clauses for AWS and CAT

Contract /SLA clauses	Included in AWS contract or SLA?	Included in CAT contract or SLA?
FAR 52-203-13—Contractors to fully cooperate by disclosing sufficient information for law enforcement purposes	Yes	Yes
FAR 52-239-1—Agency access to the CSP's facilities	Yes	Yes
Cloud Best Practices—Allowing the CSP to only make changes to the cloud environment under specific standard operating procedures agreed to by the CSP and the federal agency in the contract	Yes	Yes
FAR 52-215-2/Cloud Best Practices—OIG access to the contractor's facilities, installations, operations, documentation, databases, and personnel	Yes	No
Cloud Best Practices—Penalties for noncompliance with contract and SLA	Yes	No
Cloud Best Practices—Contract includes procedures for agencies to conduct forensic investigations	No	No
Cloud Best Practices—Addressing procedures for e-discovery when conducting a criminal investigation	No	No

Source: OIG analysis of the CFPB's AWS and CAT contracts.

CFPB officials informed us that the guidance used to develop the AWS and CAT contracts and SLAs did not include references to FAR clause 52.215-2 or the best practice clauses that we found to be missing. By ensuring that these clauses are included in cloud computing contracts and SLAs, the CFPB will have greater assurance that it will have timely access to agency information hosted in the cloud and be able to hold CSPs accountable for noncompliance with contract and SLAs.

Recommendations

We recommend that the Chief Information Officer

2. Assess the costs and benefits of negotiating post-award agreements with Amazon.com and Deloitte to include clauses for Inspector General information access, the conduct of forensic investigations and e-discovery, and penalties for noncompliance with contract and SLA terms, as appropriate.
3. Ensure that the guidance used to develop contracts and SLAs with CSPs references FAR requirements and best practice contract clauses for information access, conduct of forensic investigations and e-discovery, and penalties for noncompliance, as appropriate.
4. Ensure that future CFPB contracts for cloud computing services include FAR requirements and best practice clauses for information access, the conduct of forensic investigations and e-discovery, and the assessment of penalties for noncompliance with contract and SLA terms.

Management's Response

The Chief Information Officer concurs with recommendation 2 and is undertaking steps to assess the feasibility, as well as cost-benefit and trade-off analyses, for the existing contracts with both Amazon.com and Deloitte and, where appropriate, to execute post-award agreements to help increase assurances that the OIG has timely access to information hosted in these CSPs, and that government interests are protected appropriately.

The Chief Information Officer concurs with recommendation 3. Inclusion of standardized FAR clauses, requirements for information access in support of audit and assessments, and penalties for less-than-compliant contract execution on the part of the CSPs, are all matters that are in scope for the CFPB's ongoing supply chain guidance maturation goals and improvement processes.

The Chief Information Officer concurs with recommendation 4 and plans to develop a more robust repertoire of cloud service acquisition terms and conditions.

OIG Comment

In our opinion, the actions described by the Chief Information Officer are responsive to our recommendation. We plan to follow up on the actions to ensure that the recommendation is fully addressed.

Appendix A

Scope and Methodology

In January 2014, CIGIE initiated a government-wide review of select agencies' efforts to adopt cloud computing technologies. The initiative focused on reviewing cloud computing contracts for inclusion of specific clauses and the agencies' efforts to monitor the performance of CSPs. In support of the CIGIE initiative, our objective was to review the CFPB's acquisition and contract management for AWS and CAT to determine whether requirements for security, service levels, and access to records were appropriately planned for, defined in contracts, and being monitored.

To accomplish our audit objective, we developed an inventory of cloud computing–based systems by surveying CFPB officials responsible for the procurement, maintenance, and monitoring of the agency's cloud contracts. To perform our assessment, we judgmentally selected the AWS and CAT cloud computing–based systems based on their respective service models, contract lengths, total contract values, and associated risk categorizations. To perform our review, we analyzed the AWS and CAT contracts, SLAs, and security documentation. Further, we interviewed managers and staff at the CFPB, as well as contracting officers at Treasury who were responsible for the development of the AWS and CAT contracts.

We performed our fieldwork from February 2014 through June 2014. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B

Management's Response



September 23, 2014

Mr. Andrew Patchan, Jr.
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and C Streets, NW
Washington, DC 20551

Dear Mr. Patchan,

Thank you for the opportunity to review and comment on the Office of Inspector General's report entitled *Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services*.


We are pleased that you found that our contracts with Amazon.com and Deloitte included appropriate roles and responsibilities, information security requirements, and service-level expectations. We also appreciate your acknowledgement of the Bureau's efforts in establishing processes to monitor compliance with the contractual requirements as well as the service-level requirements of our CSP contracts.

We have reviewed the report and concur with your recommendations regarding opportunities for improvement in the areas of acquisition and contract management, specifically the manners in which sources of supply, cost analyses, inclusion of electronic discovery and investigatory forensic abilities, as well as records examination rights and noncompliance penalties, are managed in our CSP procurements. These recommendations are consistent with the Bureau's plans to mature our supply chain risk management processes, particularly in concert with the evolving standards and doctrine of the FedRAMP and NIST cloud computing endeavors.

Thank you for the professionalism and courtesy that your office demonstrated throughout this review, as well as your acknowledgement of our efforts to be responsive, communicative, and supportive of the audit team throughout the audit. We have provided comments for each recommendation.

Sincerely,

**ASHWIN
VASAN**

 Digitally signed by ASHWIN VASAN
DN: c=US, o=U.S. Government, ou=Consumer
Financial Protection Bureau, cn=ASHWIN
VASAN,
0.9.2342.19200300.100.1.1=95581002465793
Date: 2014.09.30 20:49:24 -0400'

Ashwin Vasan
Chief Information Officer

Enclosure

**Response to Opportunities for Improvement Presented in the IG Report Entitled
*Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing
Services***

Recommendation 1: Ensure that an alternatives and cost analysis is conducted to inform the selection of cloud computing service providers and models.

Management Response: The Bureau concurs with this recommendation. As noted in the report, the Bureau's current investment review process was not yet in place when the contract with Amazon.com was initially awarded early in the Bureau's history, when we were rapidly working to establish an independent IT infrastructure. The acquisition of Compliance Analysis Toolkit (CAT), as cited in the report, did undergo a business case analysis including alternative and cost analysis that lead us to the selection of that tool as provided by Deloitte. Now with the Bureau's investment review and capital investment planning processes in place, we are working to continue to mature our processes, which will include the appropriate reviews during source selection as well as cost/benefit and trade-off analyses.

Recommendation 2: Assess the costs and benefits of negotiating post award agreements with Amazon.com and Deloitte to include clauses for Inspector General information access, the conduct of forensic investigations and e-discovery, and penalties for noncompliance with contract and SLA terms, as appropriate.

Management Response: The Bureau concurs with this recommendation. Like all Federal agencies executing under the "Cloud First" policy (Federal Cloud Computing Strategy, etc.), the Bureau must contend with the marketplace variables and evolving technologies, and this is no more apparent than in the forensic and ESI (electronically stored information) discovery tools and methods. Simultaneous with that are the contractual terms and conditions that are unique to each CSP in how they accommodate access for audits and reviews, as well as compliance enforcement penalties, methods for measurement of compliance, and the remedies that can be afforded the Government in cases where compliance is found lacking. The Bureau is undertaking steps to assess the feasibility, as well as cost/benefit and trade-off analyses, for the existing contracts with both Amazon.com and Deloitte and, where appropriate, execute post-award agreements to help increase assurances that we have timely access to information hosted in these CSPs, and that Government interests are protected appropriately.

Recommendation 3: Ensure that the guidance used to develop contracts and SLAs with CSPs references FAR requirements and best practice contract clauses for information access, conduct of forensic investigations and e-discovery, and penalties for noncompliance, as appropriate.

Management Response: The Bureau concurs with this recommendation. The Bureau monitors issuances from NIST and the Federal CIO Council's FedRAMP organizations, and has noted that guidance is continuing to emerge regarding these topics. Just in September of this year, the FedRAMP program was closing the public comment period on CSP procurement topics like Incident Response and Vulnerability Scanning, in support of their issuing further requirement guidance in the future. In June of this year, the FedRAMP program issued version 2.0 of the FedRAMP Control Specific Contract Clauses, which contains further elaboration and refinement of procurement requirements for topics like Incident Response and invocation of NIST issuances on forensics and other technical

specialties. Simultaneous with that, we have observed as the marketplace continues to develop and introduce product offerings related to e-discovery and cloud ESI retrieval in support of litigation, law enforcement, and other mandates. These drivers, along with inclusion of standardized FAR clauses, requirements for information access in support of audit and assessments, and penalties for less than compliant contract execution on the part of the CSPs, are all matters that are in-scope for the Bureau's ongoing supply chain guidance maturation goals and improvement processes. Recommendation #3 supports the Bureau's objective of improving CSP procurement and execution as both the Bureau and the cloud marketplace continue to evolve.

Recommendation 4: Ensure that future CFPB contracts for cloud computing services include FAR requirements and best practice clauses for information access, the conduct of forensic investigations and e-discovery, and penalties for noncompliance with contract and SLA terms, as appropriate.

Management Response: The Bureau concurs with this recommendation. Recommendation #4 aligns precisely with our efforts related to Recommendation #3 and our plans to develop a more robust repertoire of cloud service acquisition terms and conditions. As we continue to refine CSP procurement guidance, we will leverage these improved acquisition standards in our procurements of cloud-based offerings. These will specifically address inclusion of appropriate FAR clauses, the ability to execute forensic collection and e-discovery with minimal risk of spoliation of evidentiary and legal information, the ability to access Government information in a timely manner in support of audit and assessment requirements, and appropriate penalties for anything less than compliant execution on the part of our CSP providers, including methods to assess compliance.



OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the
OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig