UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Cloud Computing

Report No. OIG-AMR-74-14-03

October 21, 2014

CORRECTED AUDIT REPORT
Corrections are identified in [ ] on pages 12-14 and 19

CONTENTS

EXECUTIVE SUMMARY 1

BACKGROUND 2

OBJECTIVE, SCOPE, AND METHODOLOGY 2

CIGIE CLOUD COMPUTING TEMPLATE 5

FINDINGS 15

Best Practices for Cloud Computing *15*
Recommendation *16*
Limitations on Services *16*
Recommendation *17*
FAR Clauses *17*
Recommendation *18*
Compliance with FedRAMP *18*
Recommendation *19*

APPENDIX

Memorandum from the Chief Financial Officer and the Chief Information Officer, Response to Audit of the National Labor Relations Board Cloud Computing Report No. OIG-AMR-74-XX-XXX, dated September 8, 2014

CORRECTED AUDIT REPORT
Corrections are identified in [ ] on pages 12-14 and 19

National Labor Relations Board
Office of Inspector General

EXECUTIVE SUMMARY

Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services. That opportunity, however, brings with it challenges and vulnerabilities.

This audit evaluates the Agency's efforts to adopt cloud computing technologies and review contracts for cloud services for compliance with applicable standards. We conducted this audit in conjunction with a Governmentwide initiative by the Council of the Inspectors General on Integrity and Efficiency. We compiled the results of our audit into a Governmentwide report.

We generally found that the Agency is using and monitoring its cloud computing services. We also noted areas where the acquisition and implementation processes would benefit from additional procedures.

The Chief Financial Officer and the Chief Information Officer provided comments on the draft report. They stated that they concurred with the report's recommendations and that the Agency is committed to acting upon them. The comments also noted that the Acquisitions Management Branch has designated Contracting Officers for information technology and cloud computing procurements and those individuals were the only representatives from the acquisitions career field at the Federal Mobile and Cloud Computing Summit in June 2014. The comments provided examples of actions that the Agency has taken to use cloud computing to maximize capacity utilization; improve flexibility and responsiveness; and minimize cost.

CORRECTED AUDIT REPORT
Corrections are identified in [ ] on pages 12-14 and 19

BACKGROUND

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for on-demand network access to shared computing resources. Cloud computing presents the Federal Government with an opportunity to transform its Information Technology (IT) portfolio by giving agencies the opportunity to focus on paying for IT services consumed rather than buying IT capacity. As a result, cloud computing helps the Government increase operational efficiencies, resource utilization, and innovation across its IT portfolio and delivers a higher return on investment to the taxpayer. Because of this potential, the U.S. Chief Information Officer instituted a "Cloud First" policy, which is intended to accelerate the pace at which the Government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

Despite the potential benefits, cloud services also have potential vulnerabilities. The vulnerabilities include the complexity of a cloud computing environment, dependency on the cloud service provider to maintain separation of an agency's data, and the need to retain appropriate control.

OBJECTIVE, SCOPE, AND METHODOLOGY

This audit's objectives were to evaluate the Agency's efforts to adopt cloud computing technologies and review contracts for cloud services for compliance with applicable standards. The audit scope was cloud computing services that the Agency used through February 2014.

We interviewed staff in the Office of the Chief Information Officer (OCIO) and the Acquisitions Management Branch (AMB) regarding the Agency's processes for acquiring and managing cloud computing services. We reviewed the Federal Acquisition Regulation (FAR) and Governmentwide guidance on cloud computing systems issued by NIST and the Office of Management and Budget (OMB). We also reviewed guidance jointly published by the Chief Information Officers Council (CIO Council) and the Chief Acquisition

Officers Council (CAO Council) regarding best practices for acquiring cloud computing services.

We obtained a listing of the Agency's cloud computing systems from the OCIO. From that listing, we selected a judgmental sample of the systems with the four largest contract values and obtained the contract files from AMB and other documentation related to the cloud computing systems from the OCIO.

For each system in the sample, we reviewed the contract files to determine whether:

- The contracts with cloud service providers clearly define the roles and responsibilities of the Agency, cloud service provider, and, if applicable, system integrators;

- The contracts with cloud service providers contain service level agreements that define performance with clear terms and definitions, demonstrate how performance is being measured, and what enforcement mechanisms are in place to ensure the service level agreements are met;

- The contracts with cloud service providers contain recommended language for allowing Agency personnel access to a cloud service provider's facilities to perform audit and investigative activities as needed;

- The Agency monitors its cloud computing providers and integrators to ensure that service level obligations are met;

- The Agency centrally manages contracts with cloud service providers to fully recognize all applicable pricing discounts; and

- The Agency's cloud service providers are compliant with the Federal Risk and Authorization Management Program (FedRAMP).

This audit was conducted in conjunction with a Governmentwide initiative by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). To perform the audit, we completed the CIGIE-provided template

questionnaire. The audit results were consolidated with the responses of other Federal agencies as a part of a CIGIE report.

We conducted this performance audit in accordance with generally accepted government auditing standards during the period February 2014 through June 2014. 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.

[CONTINUED ON FOLLOWING PAGE]

CIGIE CLOUD COMPUTING TEMPLATE

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
1.1	Date the Agency's Inspector General Contact received the completed CIGIE Cloud Computing Survey from the Agency.	February 27, 2014			
1.2	If the Agency did not return a completed survey - please provide a reason why in the response field. (*i.e.* Agency was not able to provide because it did not have any cloud systems in its inventory.)	Not Applicable			
2.1	How many total cloud IT services were identified from the survey?	6			
2.2	How many unique cloud service providers were identified from the survey?	6			
3.1	Did the Cloud contract include Terms of Service clauses?	No	No	No	Yes
3.1a	If not, did the Department/Agency sign a Terms of Service agreement with the cloud service provider?	Yes	No	No	N/A
3.2	If the Terms of Service clauses were not directly within the contract, but referenced within the contract, were the Terms of Service clauses negotiated and agreed to prior the contract being awarded?	No	N/A	N/A	N/A

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
3.3	Is there a Departmental/Agency official assigned to monitor the cloud service provider's compliance with the Terms of Service?	Yes	Yes	Yes	Yes
3.4	Is there a Departmental/Agency official assigned to monitor the Agency's compliance with the Terms of Service?	Yes	Yes	Yes	Yes
3.5	Do the Terms of Service clauses or the Cloud contract address timeframes that the cloud service provider will need to follow in order to comply with Federal agency rules and regulations?	No	No	No	No
3.6	Did the cloud service provider sign a non-disclosure agreement with the Department / Agency in order to protect non-public information that is procurement-sensitive, or affects pre-decisional policy, physical security, or other information deemed important to protect?	No	No	No	No
3.6a	If so, does the non-disclosure agreement establish rules of behavior for the cloud service provider and a method to monitor end-users activities in the cloud environment?	N/A	N/A	N/A	N/A

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
3.6b	If so, is there a Departmental/Agency official assigned to monitor the cloud service provider's compliance with the non-disclosure agreement?	N/A	N/A	N/A	N/A.
4.1	Does the Agency have an executed Service Level Agreement with the cloud service provider, either as part of the contract, or as a stand-alone document?	Yes	No	No	Yes
4.2	Does the executed Service Level Agreement for the cloud service specify required uptime percentages?	Yes	N/A	N/A	Yes
4.3	Does the executed Service Level Agreement for the cloud service describe how the uptime percentage is calculated?	Yes	N/A	N/A	Yes
4.4	Does the executed Service Level Agreement detail remedies to be paid by the cloud service provider to the Agency if the uptime requirements are not met?	Yes	N/A	N/A	Yes
4.5	Has the Department/Agency assigned someone to monitor the actual uptime, compare it to the percentage included in the executed Service Level Agreement, and pursue service credits if applicable?	Yes	N/A	N/A	Yes

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
4.6	Has the Department/Agency realized any service credits due to uptime failures?	Yes	N/A	N/A	N/A
4.7	Does the executed Service Level Agreement detail data preservation responsibilities?	Yes	N/A	N/A	Yes
4.8	Does the executed Service Level Agreement address scheduled service outages?	No	N/A	N/A	Yes
4.9	Does the executed Service Level Agreement require a service outage to be announced in advance in order not to be considered a failure to meet uptime requirements?	No	N/A	N/A	Yes
4.10	Does the executed Service Level Agreement address Service Agreement Changes?	Yes	N/A	N/A	Yes
4.11	If the cloud service provider reserves the right to modify the terms of the service agreement at any time, does the executed Service Level Agreement require the cloud service provider to provide notice of the changes to the Agency?	Yes	N/A	N/A	No

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
5.1	Does the Cloud contract, Service Level Agreement, or Terms of Service agreement, contain FAR clause 52.239-1, allowing the Agency access to the cloud service provider 's facilities, installations, technical capabilities, operations, documentation, records, and databases?	Yes	No	Yes	Yes
5.2	Does the Cloud contract, Service Level Agreement, or Terms of Service allow agencies to conduct forensic investigations for both criminal and non-criminal purposes without interference from the cloud service provider?	No	No	Yes	No
5.3	Does the Cloud contract, Service Level Agreement, or Terms of Service allow the cloud service provider to only make changes to the cloud environment under specific standard operating procedures agreed to by the cloud service provider and the Federal agency in the contract?	No	No	Yes	No

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
5.4	Does the Cloud contract, Service Level Agreement, or Terms of Service include FAR clause 52.203-13, requiring contractors fully cooperate by disclosing sufficient information for law enforcement to identify the nature and extent of the offense as well as providing timely response to Government auditors' and investigators' requests for documents and access to employees with information?	Yes	No	Yes	Yes
5.5	Does the Cloud contract, Service Level Agreement, or Terms of Service address procedures for electronic discovery when conducting a criminal investigation?	Yes	No	Yes	No
5.6	Does the Cloud contract, Service Level Agreement, or Terms of Service agreement, contain FAR clause 52.215-2, granting the Inspector General access to (i) Examine any of the Contractor's or any subcontractor's records that pertain to and involve transactions relating to this contract or a subcontract hereunder; and (ii) Interview any officer or employee regarding such transactions?	Yes	No	No	Yes

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
5.7	Does the Cloud contract, Service Level Agreement, or Terms of Service include language allowing the Office of Inspector General full and free access to the Contractor's (and subcontractor's) facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews?	No	No	Yes	No
6.1	Has the Agency designated a person responsible for monitoring the cloud service provider and/or the system integrator to verify that contractual obligations are met?	Yes	Yes	Yes	Yes
6.2	Does the Agency monitor its cloud service providers to ensure its service level obligations are met?	Yes	Yes	Yes	Yes
6.3	Does the Agency monitor its system integrator, if different from the cloud service provider, to ensure its service level obligations are met?	Yes	N/A	N/A	N/A
7.1	Does the Department/Agency have an office or group that centrally manages cloud service contracts to recognize applicable pricing discounts?	No			

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
7.1a	If so, was this office/group utilized to procure all cloud services sampled?	N/A			
7.2	Were any pricing discounts realized on the cloud services procured?	No	Yes	No	No
7.2a	If so, document the amount of savings identified into the response field.	N/A	$31,604	N/A	N/A
7.3	Was a Blanket Purchase Agreement used to procure this cloud service?	No	No	No	No
7.4	Was a GSA Cloud Blanket Purchase Agreement used to procure this cloud service?	No	No	No	No
7.5	Was the GSA IT 70 Federal Supply Schedule used to procure this cloud service?	Yes	No	No	Yes
7.6	Was a cost savings analysis performed on the use of the cloud service?	Yes	No	Yes	No
7.6a	If so, document the amount of savings identified into the response field.	$500,000 (over 6 years)	N/A	$1,000,000	N/A
8.1	Is the cloud service FedRAMP Compliant?	Yes	No	[No]	No

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
8.1a	If not, has the Agency or the cloud service provider applied to FedRAMP to initiate the assessment review?	N/A	No	[Yes]	Yes
8.1b	If not, has the cloud service provider documented its FedRAMP implemented security controls in its System Security Plan?	N/A	No	[Yes]	Yes
8.1c	If not, has the cloud service undergone an independent assessment completed by a FedRAMP approved Third Party Assessment Organization (3PAO)? (Verify if the vendor is included on the "FedRAMP Compliant 3PAO" list, included in the criteria links.)	N/A	No	[No]	No
8.1d	Specify assessment organization in response field.	N/A	N/A	[Dynamics Research Corporation]	Veris Group
8.2	Has the cloud service provider received a Provisional Authorization from the Joint Authorization Board?	N/A	No	[No]	No
8.3	Did the Agency leverage, or does it plan on leveraging, a pre-existing Provisional Authorization from a FedRAMP approved cloud service provider?	Yes	No	Yes	Yes

Question		Amazon Web Services	DiscoverText	Office 365	ServiceNow
8.3a	If so, did the Agency separately address a subset of security controls with the cloud service provider that was not documented in the Provisional Authorization originally granted by the Joint Authorization Board?	No	N/A	No	No
9.1	Does the cloud service have an authorization from the FedRAMP Joint Authorization Board?	Yes	No	[No]	No
9.2	Does the cloud service have an Authority To Operate from the Agency?	No	N/A	[N/A]	N/A

FINDINGS

Best Practices for Cloud Computing

In February 2012, the CIO Council and the CAO Council jointly published a paper titled "Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service." The paper provides Federal agencies more specific guidance in effectively implementing the "Cloud First" policy and moving forward with the Federal Cloud Computing strategy by focusing on ways to more effectively procure cloud services within existing regulations and laws. The paper is intended to be guidance developed from the best practices across government and industry for agencies to use when entering the procurement process.

The Agency entered into procurement actions for the purchase of cloud computing services that did not follow the identified best practices. These include:

- Federal agencies need to know if a cloud service provider requires an end user to agree to Terms of Service in order to use the cloud service provider's services prior to signing a contract. Terms of Service restrict the ways Federal Agency consumers can use cloud service provider environments. If the Terms of Service are not directly within the contract but referenced within the contract, they should be negotiated and agreed upon prior to contract award. Two of the four cloud services tested contained Terms of Services, one of which had a separate agreement. The separate agreement, however, was not agreed upon until after the award of the contract.

  Additionally, the terms of service must address time requirements that a cloud service provider will need to follow to comply with Federal agency rules and regulations, including statutory requirements and associated deadlines. The contract documents for the four cloud services tested did not contain these requirements.

- Federal agencies often require cloud service provider personnel to sign non-disclosure agreements when

dealing with Federal data in order to ensure that cloud service provider personnel protect non-public information that is procurement-sensitive or affects pre-decisional policy or physical security. For the four cloud services tested, the Agency did not enter into non-disclosure agreements with the cloud service provider.

- Service level agreements define acceptable service levels to be provided by the cloud service provider to its customer in measurable terms. Federal agencies should ensure that cloud service provider performance is clearly specified in all service level agreements, and that all such agreements are fully incorporated, either by full text or by reference, into the cloud service provider contract. Two of the four cloud computing services did not have an executed service level agreement.

- Federal agencies should require cloud service providers to allow forensic investigations for both criminal and non-criminal purposes, and that investigations should be conducted without affecting data integrity and without interference from the cloud service providers. Additionally, Federal agencies should ensure that cloud services providers are only allowed to make changes related to the cloud environment under specific operating procedures and have procedures for electronic discovery when conducting criminal investigations.

  For the four cloud services tested, only Office 365 contained all three best practices; Amazon Web Services contained language related to electronic discovery; and the other two cloud services did not contain any of the proposed language.

Recommendation

1. We recommend that the Chief Financial Officer establish procedures to ensure that the appropriate CIO Council and CAO Council best practices are incorporated into future procurements of cloud computing services.

Limitations on Services

The terms of services for a cloud service are determined by a legally binding agreement between the two parties contained

in a service agreement and a service level agreement. The service level agreement states the technical performance promises made by a provider, including remedies for performance failures. NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, identifies limitations that cloud service provider policies generally have, including scheduled service outages not counting as a failure to perform, and providers reserving the right to change the terms of the service agreement at any time, and to change pricing with limited advance notice. NIST recommends that if the terms of the default service agreement do not address the agency's needs, the agency should discuss modifications of the service agreement prior to use.

The Agency entered into service level agreements for two of the four cloud services tested. The service level agreements do not address the limitations addressed by NIST, as addressed below:

- The service level agreement for Amazon Web Services does not address scheduled outages and the scheduling of those outages in advance; and

- The service level agreement for ServiceNow did not address that notice be provided for changes to the agreement.

Recommendation

2. We recommend that the Chief Financial Officer establish procedures to address modifications to service level agreements when the agreements do not meet the needs of the Agency, as identified by the Chief Information Officer.

FAR Clauses

The FAR contains the following access-related clauses:

- 52.203-13, Contractor Code of Business Ethics and Conduct, which states that the contractor's internal control system shall provide for full cooperation with any Government agencies responsible for audits, investigations, or corrective actions. Full cooperation is

defined as "disclosure to the Government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to Government auditors' and investigators' request for documents and access to employees with information."

- 52.215-2, Audit and Records—Negotiation, which states that the Comptroller General, an appropriate Inspector General, or an authorized representative of either, shall have access to and the right to examine any of the Contractor's or any subcontractor's records that pertain to and involve transactions relating to this contract or a subcontract hereunder; and interview any officer or employee regarding such transactions.

- 52.239-1, Privacy or Security Safeguards, which states that "To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases."

For the four cloud services tested, Amazon Web Services and ServiceNow contained the three FAR clauses. For the two remaining contracts, one had Clauses 52.203-13 and 52.239-1, and the other did not contain any of the clauses.

Recommendation

3. We recommend that the Chief Financial Officer establish procedures to ensure that all FAR clauses related to access to cloud systems are incorporated into future procurements of cloud services.

Compliance with FedRAMP

FedRAMP is a Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The purpose of FedRAMP is to ensure that cloud based services used Governmentwide have adequate

information security, eliminate duplication of effort and reduce risk management costs, and enable rapid and cost-effective procurement of information systems / services for Federal agencies. Agencies were required to have their cloud computing systems compliant with FedRAMP by June 2014.

As of June 2014, [three] of the four cloud computing services tested were not compliant with FedRAMP. For the non-compliant services, ServiceNow [and Office 365 were] in the documentation stage of obtaining a Provisional Authorization by the Joint Authorization Board, and DiscoverText had not begun the process. We are not making a recommendation regarding this issue because it is being addressed at the Governmentwide level.

Federal agencies are required by the Federal Information Security Management Act (FISMA) to individually accept risk and grant an authority to operate before placing any agency data into a system. Agencies can use the FedRAMP provisional authorizations to grant an authority to operate for cloud systems in accordance with FISMA. Authorities to operate have not been issued by the Chief Information Officer for the four cloud computing systems tested. The Chief Information Officer concurred with this finding and noted that while the cloud service providers do not have a discrete authority to operate, Office 365 and ServiceNow are initially identified and scheduled for assessment as part of the Agency's General Support System.

Recommendation

4. We recommend that the Chief Information Officer develop procedures to ensure that Agency systems are granted an authority to operate prior to placing Agency data into the system.

APPENDIX

CORRECTED AUDIT REPORT
Corrections are identified in [ ] on pages 12-14 and 19

UNITED STATES GOVERNMENT
National Labor Relations Board
Office of the Chief Financial Officer
Memorandum

Date: September 8, 2014

To: David P. Berry
Inspector General

From: Ronald E. Crupi
Chief Financial Officer

Bryan Burnett
Chief Information Officer

Subject: Response to Audit of the National Labor Relations Board Cloud Computing Report No. OIG-AMR-74-XX-XXX

As noted in the Executive Summary of the above subject report, the Chief Financial Officer (CFO) and Chief Information Officer (CIO) concur with the Office of Inspector General's (OIG) four recommendations and are committed to acting on them.

We appreciate the Inspector General's recognition of the applicable compliance with Cloud Computing requirements as we work within the Office of the Chief Financial Officer (OCFO), Acquisitions Management Branch (AMB), in partnership with the Office of the Chief Information Officer (OCIO), to implement the Inspector General's recommendations.

AMB has realigned its designated Contracting Officers to focus on the Information Technology requirements to include cloud computing. Accordingly, the NLRB was the only Government Agency to have representatives from the Acquisition career field at the Federal Mobile & Cloud Computing Summit in June 2014. This forum recognized the need for specialization of Information Technology and Cloud Computing in the Acquisition field. Further, the AMB is working on an Acquisition Handbook which will codify the OIG's recommendations to ensure compliance with all referenced Cloud Computing requirements.

The OCIO presently is developing procedures to ensure that Agency systems are granted an authority to operate prior to placing Agency data into the system.

In this report, the OIG found that the Agency is utilizing cloud computing services. Encouraged by the Federal Government's Cloud First policy, the Agency has sought to take full advantage of

cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost. Agency efforts contained in the OIG report include:

- The Agency was an early adopter of the ServiceNow cloud Information Technology Services Management (ITSM) platform, which the Office of the CIO uses to be more transparent, provide Agency staff with multiple ways to get quality support, and as the technology enabler of its internal effectiveness initiatives.

- The Agency migrated its email repositories and services to Microsoft's cloud-based, software as a service solution, Office 365. The Agency repurposed the nearly one million dollar investment in its email infrastructure to extend the lifespan of its Next Generation Case Management (NxGen) System on-premises infrastructure, and is now using the Office 365 platform to efficiently deliver administrative systems.

- The Agency utilized Amazon's Elastic Compute Cloud to:
    - Reconstruct the NxGen case management development environment to support its agile development process.
    - Save approximately $500,000 over the next 6 years by hosting its own legacy financial data rather than utilizing a shared services provider.

Ronald Crupi Digitally signed by Ronald Crupi
DN: cn=Ronald Crupi, o=National Labor Relations Board, ou=CFO, email=rcrupi@nlrb.gov, c=US
Date: 2014.09.08 21:33:24 -04'00'

Digitally signed by BRYAN BURNETT
DN: c=US, o=U.S. Government, ou=National Labor Relations Board, cn=BRYAN BURNETT, 0.9.2342.19200300.100.1.1=63001000009719
Date: 2014.09.08 19:12:01 -04'00'

Ronald E. Crupi, Chief Financial Officer

Bryan Burnett, Chief Information Officer

Copy: Chairman
General Counsel
Deputy General Counsel