



October 14, 2014

MEMORANDUM FOR: Ellen Herbst
Chief Financial Officer and Assistant Secretary for Administration

Steve Cooper
Chief Information Officer

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

A handwritten signature in cursive script that reads "Allen Crawley".

SUBJECT: Audit of the Department's Cloud Computing Efforts Identified
Contractual Deficiencies—Final Memorandum OIG-15-001-M

The Council of Inspectors General on Integrity and Efficiency (CIGIE) initiated a government-wide review to evaluate federal agencies' efforts to adopt cloud computing technologies. The review focused on determining whether contracts that agencies have issued for cloud services comply with applicable standards. This memorandum provides our findings and recommendations regarding the OIG's cloud computing audit conducted while participating in CIGIE's government-wide review.

Background

CIGIE was statutorily established as an independent entity within the executive branch by the Inspector General Reform Act of 2008¹ to

- address integrity, economy, and effectiveness issues that transcend individual government agencies; and
- increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of inspector general.

In November 2013, CIGIE requested that agencies' Offices of Inspectors General participate in a government-wide review of the use of cloud services. Inspectors General for 20 departments and agencies opted to participate in the CIGIE review. The review involved evaluating cloud service contracts for compliance with applicable contract standards and determining the agencies' cloud service providers' (CSPs') Federal Risk and Authorization Management Program (FedRAMP²) status. The memorandum³ issued by the Federal Chief Information Officer on

¹ The Inspector General Reform Act of 2008, P.L. 110-409

² FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

December 8, 2011, required that all implemented cloud services must meet FedRAMP security authorization requirements by June 5, 2014.

Objectives, Findings, and Recommendations

Our audit objectives were to evaluate the Department's efforts to adopt cloud computing technologies and to review executed contracts between the Department's bureaus and CSPs for compliance with applicable standards. We reviewed a selection of cloud service contracts initiated between Departmental bureaus and their selected CSPs to determine if applicable contracting language and clauses were included. Our selection consisted of contracts with the Census Bureau's CSPs Akamai and GovDelivery, National Institute of Standards and Technology's (NIST's) CSPs Microsoft and ServiceNow, and National Oceanic and Atmospheric Administration's (NOAA's) CSPs Google, Inc. and Fiberlink. See appendix A for further details regarding our objectives, scope, and methodology. See table B-1, in appendix B, for the dollar value and duration for each of the selected contracts.

In the course of our audit, we found that (1) there were deficiencies in the contracts we reviewed and (2) cloud services did not comply with FedRAMP security authorization requirements.

I. Cloud-Computing Contracts Are Missing Required Clauses

While the contracts and associated documents such as service level agreements, non-disclosure agreements, and terms of service generally include the required language, we noted several deficiencies (see table B-2, in appendix B, for detailed findings). Specifically, we found:

- Four of six contracts did not contain the Commerce Acquisition Regulation (CAR)⁴ clause (CAR 1352.239-72) that allows OIG access to the contractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to carry out an inspection, investigation, audit, or other review.
- One of six contracts did not contain the Federal Acquisition Regulation (FAR) clause (FAR subsection 52.239-1) that allows an agency access to the CSP's facilities, installations, documentation, records, and databases to carry out an inspection program to safeguard against threats and hazards to the security, integrity, and confidentiality of government data.

³ Office of Management and Budget, December 8, 2011. *Security Authorization of Information Systems in Cloud Computing Environments*. Washington, DC: OMB.

⁴ These are the Department of Commerce's uniform acquisition policies and procedures, which implement and supplement the Federal Acquisition Regulation (FAR).

II. The Department's Cloud Services Are Not FedRAMP-Compliant

OMB required that all cloud services currently implemented comply with FedRAMP security authorization requirements by June 5, 2014. However, we found that only two of the cloud services associated with the contracts we reviewed⁵ met the FedRAMP deadline—they each have a FedRAMP provisional authorization to operate.⁶

Nevertheless, all cloud services associated with the contracts we reviewed have been granted authorization to operate by the respective bureaus.⁷ As a result, bureau authorizing officials should be aware of risks associated with employing the cloud services that do not meet FedRAMP requirements.⁸

Recommendations

We recommend that the Department's Chief Financial Officer and Assistant Secretary for Administration

1. Ensure that all existing and future Commerce bureau cloud service contracts appropriately include clauses from CAR 1352.239-72 and FAR subsections 52.239-1.

We also recommend that the Department's Chief Information Officer

2. Ensure that Commerce bureaus employing cloud services that do not meet FedRAMP requirements conduct effective continuous monitoring of the services' security controls in order to minimize potential risks.

We have summarized your formal response in this memorandum and included a copy as appendix C. The final memorandum will appear on the OIG website pursuant to section 8M of the Inspector General Act of 1978, as amended.

In accordance with Department Administrative Order 213-5, please provide us with your action plan within 60 days of the date of this memorandum. We appreciate the cooperation and courtesies extended to us by your staff and bureau staff during our audit. If you have any questions or concerns about this memorandum, please contact me at (202) 482-1855 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

⁵ The cloud service provided to the Census Bureau by Akamai, and one of two cloud services provided to NIST by Microsoft, comply with FedRAMP authorization requirements.

⁶ A FedRAMP provisional authorization to operate is an initial approval of the CSP's authorization package by the Joint Authorization Board (JAB) that an executive department or agency can leverage to grant a security authorization to operate for the acquisition and use of the cloud service within their agency. The FedRAMP JAB consists of the chief information officers from the Departments of Defense and Homeland Security, as well as the U.S. General Services Administration, supported by designated technical representatives from their respective member organizations.

⁷ We did not evaluate any of the bureaus' security authorization packages as part of our audit.

⁸ OMB has not issued guidance to federal agencies for dealing with CSPs whose cloud services did not meet the June 2014 deadline.

cc: Brian McGrath, Chief Information Officer, Census Bureau
Joanne Buenzli Crane, Chief Financial Officer, Census Bureau
Delwin Brockett, Chief Information Officer, NIST
George E. Jenkins, Chief Financial Officer, NIST
Zachary Goldstein, Acting Chief Information Officer, NOAA
Chris Cartwright, Acting Chief Financial Officer, NOAA
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

Summary of Agency Response and OIG Comments

In response to our draft memorandum, the Department concurred with the overall findings and recommendations. Further, the Department plans to develop a corrective action plan to adequately address the risks identified within the draft memorandum.

The Department's response is provided in appendix C.

Appendix A: Objectives, Scope, and Methodology

Our audit objectives were to evaluate the Department's efforts to adopt cloud computing technologies and to review executed contracts between the Department's bureaus and CSPs for compliance with applicable standards.

Our audit is based on participation in CIGIE's November 2013 government-wide review to evaluate federal agencies' efforts to adopt cloud computing technologies. In support of the CIGIE effort, we surveyed bureaus to identify cloud service contracts in place throughout the Department. We provided summary results of the survey to CIGIE and used survey results to establish an audit universe of 35 cloud service contracts across 6 bureaus.

Based on our knowledge of and experience with Departmental bureaus, we selected a nonstatistical sample of six cloud service contracts from three bureaus—the Census Bureau, NIST, and NOAA—for review. Our selection consisted of contracts with the Census Bureau's CSPs Akamai and GovDelivery, NIST's CSPs Microsoft and ServiceNow, and NOAA's CSPs Google, Inc. and Fiberlink.

CIGIE provided matrices (as Microsoft Excel spreadsheet workbooks) for OIGs to use for evaluating the contracts and providing audit results to CIGIE. We fulfilled specific CIGIE requests as follows:

- We obtained copies of selected contracts and supporting information and did follow-up with the bureaus to ensure we had the information needed to answer the questions in the matrices.
- Next, we used the information provided by the bureaus to complete the matrix for each contract.
- Then we sent the matrices to the bureaus on May 13, 2014, and received their comments within 3 weeks.
- After reviewing bureaus' comments, we made appropriate changes to the matrices and sent them to CIGIE, the Department's Chief Information Officer (CIO), and the CIOs of the Census Bureau, NIST, and NOAA on June 16, 2014.

CIGIE will use the results matrices provided by participating OIGs to prepare a consolidated report on the state of cloud service contracts across all agencies represented. We used the results that we provided to CIGIE as the basis for this audit report.

We conducted our field work from December 2013 to May 2014 at the Department's offices in the Washington, DC, metropolitan area. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated April 26, 2013, and 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.

Appendix B: Departmental Cloud Service Contract Details

Table B-1. Contract Value and Duration by Bureau and Cloud Service Provider

	Census Bureau CSP Akamai	Census Bureau CSP GovDelivery	NIST CSP Microsoft	NIST CSP ServiceNow	NOAA CSP Fiberlink	NOAA CSP Google, Inc.
Total contract value (millions of dollars)	2.448	2.44	9.0	1.35	7.095	4.734
Contract duration (years)	4	4	5	3	2	3

Source: OIG

Table B-2. Contract Deficiencies by Bureau and Cloud Service Provider^a

CIGIE Matrix Question	Census Bureau CSP Akamai	Census Bureau CSP GovDelivery	NIST CSP Microsoft	NIST CSP ServiceNow	NOAA CSP Fiberlink	NOAA CSP Google, Inc.
Does the Cloud contract, SLA, or TOS 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? ^b	No	Yes	Yes	No	No	No
Does the Cloud contract, Service Level Agreement (SLA), or Terms of Service (TOS) agreement, contain FAR clause 52.239-1, allowing the Agency access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases?	Yes	Yes	Yes	No	Yes	Yes

Source: CIGIE and OIG

^a A "No" response indicates a deficiency.

^b CAR 1352.239-72(h) contains this language.


Appendix C: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
Office of the Secretary
Washington, D.C. 20230

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SEP 30 2014

FROM: Ellen Herbst 
Chief Financial Officer
and Assistant Secretary for Administration

Steven I. Cooper 
Chief Information Officer

SUBJECT: Agency Response to OIG's Draft Memorandum *Cloud Computing Efforts Identified Contractual Deficiencies*

This memorandum responds to the draft memorandum from the Office of the Inspector General titled, *Cloud Computing Efforts Identified Contractual Deficiencies*. The draft memorandum identifies deficiencies in contracts for cloud services and notes that several cloud services provided to the Department did not comply with Federal Risk and Authorizations Management Program (FedRAMP) security requirements. The Department concurs with the overall findings and recommendations outlined within the draft memorandum.

Further, the Department will develop and submit a corrective action plan to adequately address the risks identified within the OIG's draft memorandum.

cc: Brian McGrath, Chief Information Officer, Census Bureau
Joanne Buenzil Crane, Chief Financial Officer, Census Bureau
Delwin Brockett, Chief Information Officer, NIST
George E. Jenkins, Chief Financial Officer, NIST
Zachary Goldstein, Acting Chief Information Officer, NOAA
Chris Cartwright, Acting Chief Financial Officer, NOAA

01120000176