U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

EPA Is Not Fully Aware of the Extent of Its Use of Cloud Computing Technologies

Report No. 14-P-0323 **July 24, 2014**

Scan this mobile code to learn more about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Albert E. Schmidt

Abbreviations

3PAO	Third-Party Assessment Organization
BPA	Blanket Purchase Agreement
CFR	Code of Federal Regulations
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CO	Contracting Officer
CSP	Cloud Service Provider
eNOI	Electronic Notice of Intent
EPA	U.S. Environmental Protection Agency
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FY	Fiscal Year
GSA	General Services Administration
IM/IT	Information Management/Information Technology
IT	Information Technology
N/A	Not applicable
NCC	National Computer Center
NDA	Nondisclosure Agreement
NIST	National Institute of Standards and Technology
NOI	Notice of Intent
OAM	Office of Acquisition Management
OEI	Office of Environmental Information
OIG	Office of Inspector General
PMOS	Permit Management Oversight System
SLA	Service Level Agreement
SP	Special Publication
TOS	Terms of Service

U.S. Environmental Protection Agency
Office of Inspector General

14-P-0323
July 24, 2014

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to evaluate select agency efforts to adopt cloud computing technologies and to review executed contracts between the agency and cloud service providers for compliance with applicable standards. This audit was conducted as part of a governmentwide initiative by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Information gathered during the subject audit will be incorporated into a governmentwide report to be released by CIGIE.

The report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization*.

For further information, contact our public affairs office at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2014/20140724-14-P-0323.pdf

EPA Is Not Fully Aware of the Extent of Its Use of Cloud Computing Technologies

What We Found

EPA officials lack confidence that offices recognize its full use of cloud computing for agency operations.

The CIGIE developed a survey and asked its members to contact their respective agencies and collect information about the deployment of cloud computing technologies. Additionally, CIGIE provided a matrix template for each Inspector General to complete to standardize the results of the CIGIE collaboration effort, and to assist with the completion of the consolidated report. In consultation with the CIGIE, the EPA OIG selected one system to review and completed the provided matrix with test results.

The EPA OIG selected the current contract for the Office of Water's Permit Management Oversight System (PMOS) for testing. In 2012, the Office of Water used the Office of Acquisition Management to contract for a vendor to maintain and host the PMOS application. Although the PMOS was not included in the EPA's response document to the CIGIE survey, the PMOS is currently hosted by an EPA subcontractor whose hosting environment has cloud characteristics. The subcontractor's hosting environment also appeared to meet the definition of a "cloud," as defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145, *The NIST Definition of Cloud Computing*.

The PMOS enables the EPA to track general and tribal permits at a summary level. The PMOS captures limited information on these permits, which enables the EPA to track the universe and status of these permits. The PMOS is used to prepare National Pollutant Discharge Elimination System reports for the Office of Management and Budget.

Our audit work disclosed management oversight concerns regarding the EPA's use of cloud computing technologies. These concerns highlight the need for the EPA to strengthen its catalog of cloud vendors and processes to manage vendor relationships to ensure compliance with federal security requirements. In particular:

- The EPA did not know when its offices were using cloud computing.
- The EPA should improve the oversight process for prime contractors (to include ensuring subcontractors comply with federal security requirements and establishing service-level agreements for cloud services).
- There is no assurance that the EPA has access to the subcontractor's cloud environment for audit and investigative purposes.
- The subcontractor is not compliant with the Federal Risk and Authorization Management Program.

The EPA indicated the provided matrix is factually correct. The EPA response and our comments are at appendix B.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

July 24, 2014

MEMORANDUM

SUBJECT: EPA Is Not Fully Aware of the Extent of Its Use of Cloud Computing Technologies
Report No. 14-P-0323

FROM: Arthur A. Elkins Jr.

TO: Rod DeSmet
Deputy Assistant Inspector General for Audit
Office of Inspector General (USDA)
CIGIE Cloud Computing Consolidated Report Lead

Attached please find the results of the subject audit. We performed this audit in accordance with generally accepted government auditing standards. Those standards require the team to plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the findings and conclusions based on the objectives of the audit.

We believe the evidence obtained provides a reasonable basis for our findings and conclusions and, in all material respects, meets the reporting requirements prescribed by Council of the Inspectors General on Integrity and Efficiency (CIGIE). In accordance with CIGIE reporting instructions, we are forwarding this report to you.

We briefed agency officials on the results of our audit work and, where appropriate, made an adjustments. The results have been verified for accuracy in accordance with our internal quality control process. As part of our process, we were unable to identify a complete audit universe via data call. Of the known cloud systems, we selected the EPA Office of Water's Permit Management Oversight System Application using non-statistical sampling.

Prior to starting work on this audit, we were in the process of performing a cloud audit related to two of the EPA's cloud initiatives. During that separate audit, we collected information that made us aware of two cloud initiatives within other program offices. Since we selected two cloud initiatives from the EPA Office of Environmental Information during the other audit, we selected one of the initiatives from a different program office to not overburden the EPA Office of Environmental Information.

The EPA offices having primary responsibility for the issues evaluated in the report are the Office of Water and Office of Administration and Resources Management's Office of Acquisition Management.

We will post this report to our website at http://www.epa.gov/oig.

Table of Contents

Appendices

Overview of the CIGIE Cloud Computing Collaboration Results Matrix	

Purpose	The purpose of the matrix is to standardize the results of the Council of Inspectors General on Integrity and Efficiency (CIGIE) collaboration effort to assist with the completion of the consolidated report.

Instructions	Provide responses to the questions in the matrix. Complete one matrix per system tested. You should design your testing to address the questions specified within each step. Each step has its own tab within the matrix. The response options include Yes, No, or N/A and are available in a drop-down list within the cell. If more than a Yes, No, or N/A is necessary for the question, we have included instructions to place the specific information in the "IG Comments" field. Additionally, please feel free to include any additional comments that are warranted.

Criteria	When possible, we have included references to criteria for the applicable steps.

Modifications	If during the course of completing the matrix, the auditor identifies a potential improvement to the matrix, please notify the following individual for requested modifications: ***Corey Bidne, Senior Auditor, USDA-OIG*** ***corey.bidne@oig.usda.gov*** ***816.823.3884***

Agency Point of Contact (Complete for the Individual in charge of testing)	
Name	Rudolph M. Brevard
Department	Office of the Inspector General (OIG)
Agency	Environmental Protection Agency (EPA)
Phone	(202) 566-0893
Email	brevard.rudy@epa.gov

The matrix is divided into tabs based on the following sections. You should design your testing to address the questions specified within each tab.	
Step 1	Cloud Data Call
Step 2	Cloud System Inventory
Step 3	Cloud Service Agreements (TOS, NDAs)
Step 4	Cloud Service Level Agreements
Step 5	Cloud Service Access
Step 6	Cloud Service Provider Monitoring
Step 7	Cloud Service Central Management
Step 8	FedRAMP Compliance Progress

Procedure Step:	**1. Cloud Computing Data Call**
Purpose*:*	Request data on agency cloud computing practices for the review of the agency's cloud computing technologies.
Scope/Methodology*:*	Submit the CIGIE Cloud Computing Survey to the agency and request data on current fiscal year (FY 2014) cloud computing systems for the review of the agency's cloud computing technologies.

Agency:	EPA
System:	

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Audit Step #	Question to Address	Response	IG Comments	Agency Response
1.1	Date the agency's inspector general contact received the completed CIGIE Cloud Computing Survey from the agency ? (mm/dd/yyyy)	February 19, 2014	N/A	
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.)	N/A—The agency returned the survey.	N/A	

Procedure Step:	**2. Inventory of Cloud Services and Service Providers**
Purpose*:*	Determine the agency's enterprise-wide inventory of cloud IT services and service providers, and select a sample of providers to evaluate
Source:	Compile the results of questionnaires sent to the department/agency Chief Information Officers (CIOs).
Scope/Methodology*:*	Determine the department/agency's enterprise-wide inventory of cloud IT services and service providers as of the survey date (FY 2014) and select a sample of providers for evaluation.

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Audit Step #	Question to Address	Response	IG Comments
2.1	How many total cloud IT services were identified from the survey (list numerical value of services in response field, limited to 2 digits)	11	The auditor lacks confidence there were 11 cloud IT services as identified in the completed cloud survey. Specifically, the Office of Acquisition Management (OAM) indicated that the Cloud Survey was completed by performing a search for the word "cloud" in the procurement description. As a result, the auditor concludes that regardless of whether a contract was a cloud contract, the contract would only be included on the list if the term "cloud" appeared in the description of the procurement. During the audit, the auditor became aware of one application incorrectly listed as a cloud application and two applications that appear to be cloud applications not included in the survey results. The OAM said it has no database that specifically identifies "cloud" procurements.
2.2	How many unique cloud service providers were identified from the survey (list numerical value of services in response field, limited to two digits).	10	

Procedure Step:	3. Roles and Responsibilities Defined in Contracts
Purpose:	Determine if the agency's contracts with cloud service providers clearly define the roles and responsibilities of the agency, the Cloud Service Provider (CSP) and, if applicable, system integrators.
Scope/Methodology:	Review selected contracts that have been executed between the agency and the CSP/Reseller and determine whether the contract contains clearly defined roles for the agency, the CSP and any system integrators
Note:	If the contract was procured through the General Services Administration (GSA) IT 70 Federal Supply Schedule (FSS), a GSA blanket purchase agreement (BPA), or a shared service BPA, when reviewing the contract, be sure to include the original contract and solicitation documentation that was agreed to by GSA or the BPA originating agency in your review to ensure all contract documentation is reviewed prior to making a determination on the results of your audit testing.
Supplement:	A supplemental guide was created to assist the auditor with identifying the additional terms, conditions, and clauses. The guide is titled "***CIGIE Audit Results Matrix Supplement-IT 70 Schedule Clauses.docx***."

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Audit Step #	Question to Address	Response	IG Comments
3.1	Did the Cloud contract include Terms of Service (TOS) clauses? (Cloud Best Practices Bookmark 5)	No	The contract indicates the primary contractor will host the Permit Management Oversight System (PMOS) application and will follow the EPA's policies and procedures; however, there are no specific Terms of Service (TOS) clauses related to the hosting of the PMOS application (We reviewed the contract, amendment, and task orders). Additionally, the EPA has not agreed to terms of service outside of the contract. On April 30, 2014, the EPA said the primary contractor agreed to the service agreement of the subcontractor responsible for hosting the PMOS and provided a link to the service agreement that included the following disclaimer: "You acknowledge and agree that your use of the services is solely at your own risk, and that except as expressly provided herein the services are provided on an 'as is' and 'as available' basis. [The subcontractor hosting the PMOS application] expressly disclaims any and all warranties and conditions of any kind, express, implied, or statutory, including, without limitation, the implied warranties of title, noninfringement, merchantability, and fitness for a particular purpose and any warranties arising from a course of dealing, usage or trade practice.

			Furthermore, [the subcontractor hosting the PMOS application] does not warrant that the services and/or any information obtained thereby shall be complete, accurate, uninterrupted, secure or error free. [The subcontractor hosting the PMOS application] further makes no warranty that the services will meet your requirements, nor does [the subcontractor hosting the PMOS application] make any warranty as to the results that may be obtained from the use of the services."
3.1a	If not, did the department/agency sign a TOS agreement with the cloud service provider?	No	The EPA has not agreed to TOS outside of the contract.
3.2	If the TOS clauses were not directly within the contract, but referenced within the contract, were the TOS clauses negotiated and agreed to prior the contract being awarded? (Cloud Best Practices Bookmark 1)	No	There were no TOS agreed to within or outside the contract related to the hosting of the PMOS application between the EPA and the primary vendor; however, as identified in audit step 3.1, the prime contractor did accept the TOS with the subcontractor. The contracting officer said they only became aware of the subcontractor as a result of audit inquiries.
3.3	Is there a departmental/agency official assigned to monitor the cloud service providers compliance with the TSO?	No	There are no TOS between the EPA and the primary contractor related to hosting the PMOS application.
3.4	Is there a departmental/agency official assigned to monitor the agency's compliance with the TOS?	No	There are no TOS between the EPA and the primary contractor related to hosting the PMOS application.
3.5	Do the TSO clauses or the cloud contract address timeframes that the CSP will need to follow in order to comply with federal agency rules and regulations? (Cloud	No	There are no TOS between the EPA and the primary contractor related to hosting the PMOS application.

	Best Practices Bookmark 2)		
3.6	Did the cloud service provider sign a nondisclosure agreement (NDA) 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? (Cloud Best Practices Bookmark 3)	No	The cloud service provider (CSP), a subcontractor, did not sign a nondisclosure agreement (NDA), but instead only had a service agreement with the primary contractor. This service agreement contains a warranty disclaimer that states: [The sub-contractor hosting the PMOS application] "does not warrant that the services and/or any information obtained thereby shall be complete, accurate, uninterrupted, secure or error free." Since the prime contractor accepted the terms of the CSP, there is no NDA between the EPA and the CSP.
3.6a	If so, does the NDA establish rules of behavior for the CSP and a method to monitor end-users activities in the cloud environment? (Cloud Best Practices Bookmark 4)	No	The EPA does not have an NDA established for the CSP; therefore, no rules of behavior were established for the CSP associated with a nondisclosure agreement. Although no nondisclosure agreement or associated rules of behavior exist for the CSP (a subcontractor), the blanket purchase agreement (BPA or contract) established rules of behavior for the primary contractor. However, we reviewed and determined that the PMOS BPA, related task orders, and modifications did not provide a method to monitor end-user activities.
3.6b	If so, is there a departmental/agency official assigned to monitor the cloud service providers compliance with the NDA?	No	The EPA does not have an official assigned to monitor CSP compliance with the NDA. The contracting officer said they are unaware of an official assigned to monitor CSP compliance with the NDA.

Procedure Step:	4. Service Level Agreements in Contracts
Purpose*:*	Determine if the agency's contracts with cloud service providers contain service level agreements (SLAs) that define performance with clear terms and definitions, demonstrate how performance is being measured, and what enforcement mechanisms are in place to ensure SLAs are met;
Scope/Methodology*:*	Review service level agreements with cloud providers and determine whether the SLA: 1. Defines performance with clear terms and definitions (uptimes, etc.) 2. Demonstrates how performance is being measured 3. Defines enforcement mechanisms when performance is not met
Note:	If the contract was procured through the GSA IT 70 Federal Supply Schedule (FSS), a GSA BPA, or a shared service BPA, when reviewing the contract, be sure to include the original contract and solicitation documentation that was agreed to by GSA or the BPA originating agency in your review to ensure all contract documentation is reviewed prior to making a determination on the results of your audit testing.
Supplement:	A supplemental guide was created to assist the auditor with identifying the additional terms, conditions, and clauses. The guide is titled "***CIGIE Audit Results Matrix Supplement-IT 70 Schedule Clauses.docx***."

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Audit Step #	Question to Address	Response	IG Comments
4.1	Does the agency have an executed service level agreement (SLA) with the CSP, either as part of the contract, or as a stand-alone document?	No	The EPA does not have an SLA. The EPA does have performance work statements (specified in the BPA), which provide the scope of work for the PMOS. Task orders have Performance Standards and Quality Assurance Surveillance Plans. However, neither the performance work statements, nor the task orders that have Performance Standards and Quality Assurance Surveillance Plans, provided detailed service levels for contractors to uphold with regard to hosting the PMOS application. These documents only state the vendor is to host the application but do not specify any service levels for contractors to uphold with regard to hosting. Additionally, as noted

			in audit step 3.1, the prime contractor agreed to the subcontractor's service agreement that contained a disclaimer on any and all warranties.
4.2	Does the executed SLA for the cloud service specify required uptime percentages?(NIST SP 800-146, 3.1)	No	The auditor reviewed and concluded that there are no SLAs that specify required uptime percentages for the PMOS in the EPA's performance work statements specified in the BPA, or in the task orders that have Performance Standards and Quality Assurance Surveillance Plans.
4.3	Does the executed SLA for the cloud service describe how the uptime percentage is calculated? (NIST SP 800-146, 3.1)	No	There are no uptime requirements for PMOS.
4.4	Does the executed SLA detail remedies to be paid by the CSP to the agency if the uptime requirements are not met? (NIST SP 800-146, 3.1)	No	There are no uptime requirements for PMOS.
4.5	Has the department/agency assigned someone to monitor the actual uptime, compare it to the percentage included in the executed SLA, and pursue service credits if applicable? (NIST SP 800-146, 3.1)	No	There are no uptime requirements for PMOS.
4.6	Has the department/agency realized any service credits due to uptime failures?	No	There are no uptime requirements for PMOS.
4.7	Does the executed SLA detail data preservation responsibilities? (NIST SP 800-146, 3.1)	Yes	The auditor reviewed and concluded that the BPA indicates: • "Once the prototype's requirements are stable, the system will be brought in line with EPA's Architecture."… • "Unless specified elsewhere in this contract, title to items furnished in the contract shall pass to the Government upon acceptance, regardless of when or where the Government takes possession." Task orders related to the PMOS indicate the contractor shall use a Microsoft Access format to perform two backups per month of the files with priority permit status.

4.8	Does the executed SLA address scheduled service outages? (NIST SP 800-146, 3.2)	No	SLAs that address scheduled service outages are not addressed in the performance work statements specified in the BPA, or in the task orders that have Performance Standards and Quality Assurance Surveillance Plans.
4.9	Does the executed SLA require a service outage to be announced in advance in order not to be considered a failure to meet uptime requirements?	No	There are no uptime requirements for PMOS.
4.10	Does the executed SLA address service agreement changes? (NIST SP 800-146, 3.2)	No	The PMOS BPA (EP-BPA-12-C-0010) does contain a change clause that states: "Changes in the terms and conditions of this contract may be made only by written agreement of the parties." However, the service agreement between the prime contractor and the subcontractor hosting the application indicates the cloud service provider can make unilateral changes to the terms of the service agreement by posting to its website.
4.11	If the CSP reserves the right to modify the terms of the service agreement at any time, does the executed SLA require the CSP to provide notice of the changes to the agency?	Yes	The PMOS BPA (EP-BPA-12-C-0010) contains a change clause that states: "Changes in the terms and conditions of this contract may be made only by written agreement of the parties;" However, unbeknownst to EPA, the service agreement between the prime contractor and the subcontractor hosting the application indicates the cloud service provider can make unilateral changes to the terms of the service agreement by posting to the subcontractor's website.

Procedure Step:	5. Access to CSP for Audit and Investigative Purposes
Purpose*:*	Determine if contracts with cloud service providers (CSPs) contain recommended language for allowing agency personnel access to CSP facilities to perform audit and investigative activities as needed.
Scope/Methodology*:*	Review selected contracts with CSPs and determine whether they contain the recommended Federal Acquisition Regulation (FAR) clauses for access to CSP facilities and specific details addressing investigative, forensic and audit access.
Note:	If the contract was procured through the GSA IT 70 Federal Supply Schedule (FSS), a GSA BPA, or a shared service BPA, when reviewing the contract, be sure to include the original contract and solicitation documentation that was agreed to by GSA or the BPA originating agency in your review to ensure all contract documentation is reviewed prior to making a determination on the results of your audit testing.
Supplement:	A supplemental guide was created to assist the auditor with identifying the additional terms, conditions and clauses. The guide is titled "***CIGIE Audit Results Matrix Supplement-IT 70 Schedule Clauses.docx***."

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Criteria:

FAR 52.239-1(b)	(b) 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.
FAR 52.203-13(a)(1)	"Full cooperation"— (1) Means 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;

FAR 52.215-2 (d)(1)

General. (1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials, shall haveaccess to and the right 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.

Cloud Best Practices:

https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

The Cloud Best Practices is a joint publication between the CIO Council and the Chief Acquisition Officers Council - we have included these benchmarks for cloud contracts within our testing because the paper was created with the intention of being "the next step in providing 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."

Audit Step #	Question to Address	Response	IG Comments
5.1	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	The contract between the prime contractor and the EPA contains the FAR clause 52.239-1 [48 CFR 52.239-1] via the applicable GSA Federal Supply Schedule Contract. However, the prime contractor agreed to the service agreement of the subcontractor hosting the application, and this agreement does not contain the FAR clause 52.239-1. The agreement contains language that would prevent the prime contractor from imposing clauses found in the EPA's contract with the prime contractor on the subcontractor.
5.2	Does the cloud contract, SLA, or TOS allow agencies to conduct forensic investigations for both criminal and non-criminal purposes without affecting data integrity and without interference from the	No	For the PMOS BPA, task orders, and modifications, the PMOS contract did not contain language that allows the EPA to conduct forensic investigations for both criminal and non-criminal purposes without interference from the CSP.

	CSP? (Cloud Best Practices, Pg. 15, Forensics)		
5.3	Does the cloud contract, SLA, or TOS allow 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? (Cloud Best Practices, Pg. 15, Forensics)	No	For the PMOS BPA, task orders, and modifications, the PMOS contract, SLA, or TOS did not contain language to restrict the CSP to only making changes to the cloud environment under specific standard operating procedures agreed to by the CSP and the EPA in the contract.
5.4	Does the cloud contract, SLA, or TOS 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 auditor and investigator requests for documents and access to employees with information? (FAR 52.203-13 (a)(1))	Yes	The contract between the prime contractor and the EPA contains the FAR clause 52.203-13 [48 CFR 52.203-13] via the applicable GSA Federal Supply Schedule Contract. However, the prime contractor agreed to the service agreement of the subcontractor hosting the application and this agreement does not contain the FAR clause 52.203-13. The agreement contains language that would prevent the prime contractor from imposing clauses found in the EPA's contract with the prime contractor on the subcontractor.
5.5	Does the cloud contract, SLA, or TOS address procedures for electronic discovery when conducting a criminal investigation?	No	For the PMOS BPA, task orders, and modifications, the PMOS contract did not contain language to address procedures for electronic discovery when conducting a criminal investigation.
5.6	Does the cloud contract, service level agreement (SLA), or Terms of Service (TOS) agreement, contain FAR clause 52.215-2, granting the Inspector General access to: (i) Examine any of the contractor's or any	No	For the PMOS BPA, task orders, and modifications, the contract between the prime contractor and the EPA does not contain FAR clause 52.215-2 [48 CFR 52.215-2].

	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?		
5.7	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?	No	For the PMOS BPA, task orders, and modifications, the PMOS contract, SLA, or TOS did not include language that allows the Office of Inspector General full and free access to contractor and subcontractor facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations or other reviews.

Procedure Step:	6. Review the Agency's Process for Monitoring Its Cloud Computing Provider
Purpose:	Determine whether the agency monitors its cloud computing providers (and if applicable integrators) to ensure they meet service level obligations.
Scope/Methodology:	Review the cloud service documentation for the selected contracts, conduct interviews with applicable personnel and compare with recommended best practices for contract and service level agreement monitoring to determine whether the agency has a process in place to effectively manage its cloud computing providers to ensure they meet their contractual obligations.

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Audit Step #	Question to Address	Response	IG Comments
6.1	Has the agency designated a person responsible for monitoring the cloud service provider (CSP) and/or the system integrator to verify that contractual obligations are met?	Yes	The agency designated a Task Order Contract Officer Representative, who is responsible for monitoring the system integrator (the prime contractor) to verify that contractual obligations are met.
6.2	Does the agency monitor its cloud service provider to ensure its service level obligations are met?	No	The agency does not have a service level agreement associated with the contract reviewed.
6.3	Does the agency monitor its system integrator, if different from the CSP, to ensure its service level obligations are met?	No	The agency does not have a service level agreement associated with the contract reviewed.

Procedure Step:	**7. Enterprise Management of Cloud Service Providers**
Purpose:	Determine if the department/agency centrally manages contracts with cloud service providers to fully recognize all applicable pricing discounts.
Scope/Methodology:	Interview applicable personnel and review applicable documentation to determine if the department/agency centrally manages contracts with cloud service providers to fully recognize all applicable pricing discounts.

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Audit Step #	Question to Address	Response	IG Comments
7.1	Does the department/agency have an office or group that centrally manages cloud service contracts to recognize applicable pricing discounts?	No	The EPA does not have an office or a group that centrally manages cloud service contracts. Management of contracts (including cloud services) is shared between an individual program office and the agency's OAM.
7.1a	If so, was this office/group utilized to procure all cloud services sampled?	No	Management of the procurement of contracts (including cloud services) is shared between a program office and the OAM.
7.2	Were any pricing discounts realized on the cloud services procured?	No	The summary price sheet for the EPA's BPA with the prime contractor indicates the base year's quoted rates are from the prime contractor's GSA contract. Additionally, there is a 3 percent annual escalation for the option years, because the prime contractor had to estimate what the actual GSA rates would be for the years beyond the base year, and because the prime contractor's GSA contract specifies that escalation is based on the Department of Labor's employment cost index.
7.2a	If so, document the amount of savings into the response field.	N/A	
7.3	Was a blanket purchase agreement (BPA) used to procure this cloud service?	Yes	There was a BPA used to procure this cloud service. The BPA was for technical support services, not cloud services. There is no use of cloud services in the BPA. A subcontractor was providing cloud services.
7.4	Was a GSA cloud BPA used to procure this cloud service?	No	Although the EPA said GSA schedule holders were solicited for cloud service, the BPA was for technical support services and not cloud services. A subcontractor was providing cloud services.

7.5	Was the GSA IT 70 Federal Supply Schedule (FSS) used to procure this cloud service?	No	Although EPA indicated that GSA schedule holders were solicited for the EPA's BPA for the PMOS contract; the GSA IT 70 Federal Supply Schedule was not used to procure the PMOS cloud service. Additionally, the Subcontractor that was providing the cloud service, was not included on the GSA schedules.
7.6	Was a cost savings analysis performed on the use of the cloud service?	No	There was no cost savings analysis done.
7.6a	If so, document the amount of savings identified into the response field.	N/A	Since there was not a cost savings analysis done, there are no identified savings to document

Procedure Step:	**8. FedRAMP Compliance**
Purpose:	Determine the progress of the cloud service and cloud service provider (CSP) in obtaining FedRAMP compliance for the system/service implemented.
Source:	Verification with FedRAMP portals, cloud service document review, and interviews with applicable personnel.
Scope/Methodology:	For the cloud services selected, review evidence of FedRAMP compliance submitted by the agency.

Prepared By:	Albert E. Schmidt
Reviewed By:	Charles M. Dade

Criteria:
FedRAMP Reference Guide: http://www.gsa.gov/portal/mediaId/170599/fileName/Guide_to_Understanding_FedRAMP_042213
FedRAMP Compliance Steps: http://www.gsa.gov/portal/category/102999
FedRAMP Compliant CSP: http://www.gsa.gov/portal/content/131931
FedRAMP Compliant 3PAO: http://www.gsa.gov/portal/content/131991
FedRAMP Contract Clauses: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Standard_Contractual_Clauses_062712.pdf
FedRAMP Concept of Operations: http://www.gsa.gov/portal/mediaId/154239/fileName/CONOPS_V12_072712
FedRAMP Sec Controls Preface: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_072912.zip
FedRAMP Baseline Sec Controls: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_072912.zip

Audit Step #	Question to Address	Response	IG Comments
8.1	Is the cloud service FedRAMP compliant?	No	The EPA's CSP was not included in the GSA's Federal Risk and Authorization Management Program (FedRAMP) listing. The OAM said the purpose of the PMOS procurement order was: "Not to procure Cloud services, rather the order was placed for technical support services in support of existing systems as follows: develop, maintain, and revise the eNOI and NOI Processing Systems, modify the eNOI system to accommodate new permits, provide regional, state, and public access to permit documents, data, and posting support, develop system training tools, and track permit priority and backlog. Per the afore-mentioned excerpt from the Performance Work Statement,

			there is no mention of a cloud services requirement. In response to the solicitation, vendors were required to offer their best technical solution for completing the above tasks, and [the prime contractor] offered a technical solution that included the cloud. Since the requirement was not for Cloud services, there was no reason for the contract to contain terms and conditions specifically on the performance of cloud services." Although, the EPA did not intend to procure a cloud service, the agency accepted a contract whose technical solution included the cloud. As a result, the auditor concludes that the contract should have included terms and conditions specifically on the performance of cloud services for those parts of the contract hosted in the cloud. Additionally, OAM stated that "the cloud services part of the technical solution was performed by a subcontractor to the prime awardee." As a result, the OAM believed that "per FAR 42.505 the EPA has no privity of contract with a subcontractor. Accordingly, the reason [OAM does] not 'appear to have any oversight or control' over the subcontractor's activities is because [OAM is] legally precluded from such a relationship." The EPA's Required Practices Concerning Subcontracts indicates the following: "Before consenting to a subcontract, the [contracting officer] CO reviews the request and supporting data and considers such factors as: technical need for services, compliance with the prime contract's goals for subcontracting with small disadvantaged business and women-owned business concerns, adequacy of competition, responsibility of the proposed subcontractor, proposed type and terms and conditions of the subcontract, and adequacy and reasonableness of cost or price analysis performed. The project officer reviews the prime contractor's request for subcontract consent, and provides comments to the CO on the technical need and appropriateness of the supplies or services, the reasonableness of the subcontract estimate in terms of level of effort, and types and quantities of proposed other direct costs; location, duration, number of travelers and purpose of proposed travel; skill level, labor mix, and direct labor hours to be expended; and the capabilities of the proposed subcontractor." As a result, the auditor concludes that the CO should only consent to subcontractors for hosting services, if the subcontractor meets the necessary federal security requirement.

8.1a	If not, has the agency or the CSP applied to FedRAMP to initiate the assessment review?	No	Per the CO, the EPA has not pursued any actions regarding the FedRAMP and the subcontractor. In fact, the subcontractor is responsible for hosting the Permit Management Oversight System (PMOS) application and has a service agreement with the prime contractor, which includes a disclaimer wherein the subcontractor states that it "does not warrant that the services and/or any information obtained thereby shall be complete, accurate, uninterrupted, secure or error free."
8.1b	If not, has the CSP documented its FedRAMP implemented security controls in its System Security Plan?	No	Per the contracting officer, the EPA has not pursued any actions regarding the FedRAMP and the subcontractor. In fact, the subcontractor is responsible for hosting the PMOS application and has a service agreement with the prime contractor, which includes a disclaimer wherein the subcontractor states that it "does not warrant that the services and/or any information obtained thereby shall be complete, accurate, uninterrupted, secure or error free."
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)	No	Per the contracting officer, the EPA has not pursued any actions regarding the FedRAMP and the subcontractor. Additionally, a subcontractor representative said the cloud service has not undergone an independent assessment by a FedRAMP-approved Third-Party Assessment Organization.
8.1d	Specify assessment organization in response field	N/A	The EPA's cloud service has not undergone an independent assessment by a FedRAMP-approved Third-Party Assessment Organization.
8.2	Has the cloud service provider received a provisional authorization from the Joint Authorization Board?	No	Per the contracting officer, the EPA has not pursued any actions regarding the FedRAMP and the subcontractor. Additionally, the subcontractor is not found on the listing of CSPs that received provisional authorization from the Joint Authorization Board.
8.3	Did the agency leverage, or does it plan on leveraging, a pre-existing provisional authorization from a FedRAMP-approved CSP?	Yes	The EPA has a contract with a vendor for Infrastructure-as-a-Service. The vendor is included on the listing of FedRAMP-compliant CSPs with a provisional authorization to operate.
8.3a	If so, did the agency separately address a subset of security controls with the CSP that was not documented in the Provisional Authorization originally granted by the JAB?	Yes	The EPA issued an authorization to operate for the Infrastructure-as-a-Service cloud vendor contract. The authorization to operate indicated the security authorization of the information system will remain in effect as long as the conditions exist as follows: 1. The vulnerabilities reported during the continuous monitoring process do not increase agency-level risk to levels deemed unacceptable.

			2. The system has not undergone any major changes requiring the system security plan to be updated. 3. The system's owner commits to complete any plan of actions and milestone that are established now or in the future to ensure the continued effectiveness of the system security plan and the security controls specified.

CIGIE Cloud Computing Survey Returned by the EPA

This page intentionally left blank

								FIPS 199 security category by type									
Department/Agency	IT Service Name	IT Application Name	Description of Service	Cloud Service Provider Name	Reseller (If Applicable)	Type (Iaas, SaaS, PaaS, Naas)	Cloud Service Model (Private, Public, Community, Hybrid)	C	I	A	Date Contract Initated	Contract Length (Base + Option Years)	Total Contract Value	Signed Service Level Agreement (SLA)	Contracting Officer's Representative	Contracting Officer	System Point of Contact	Contract Award ID
EPA			AIM SYSTEM HOSTED IN CLOUD	INSIGHT PUBLIC SECTOR, INC.		Procurement cancelled	This contract ($5,000) with Insight to host AIM application in Cloud was canceled in February 2011 due to some disagreement between OPPT and Microsoft Cloud hosting service. The requested information for AIM system hosted in Cloud is not available.				6/8/2011	3 Years	$5,958.72	Procurement cancelled	Susan Lei	Genine McElroy		EPG11H00143
EPA			MICROSOFT OFFICE 365 CLOUD SERVICES	DELL FEDERAL SYSTEMS L.P.			Microsoft Office 365 (Office 2013) cloud service and support for 18,000 licenses, includes maintenance, future upgrades, and patches.				6/19/2013	5 Years	$7,905,600.00		Gloria Meriweather	Deborah Darry		EPG13H00710
EPA			THIS 0365 OFFICE PROVIDES FOR MAINTENANCE AND UPGRADES FROM THE CLOUD. MUST BE PURCHASED BY JUNE 14TH. PAYMENT WILL BE DUE 45 DAYS AFTER INVOICING.	DELL MARKETING LIMITED PARTNERSHIP			Microsoft Office 365 (Office 2013) cloud service and support for 18,000 licenses, includes maintenance, future upgrades, and patches.				7/11/2013	5 Years	$7,905,600.00		Gloria Meriweather	Deborah Darry		EPG13H00714
EPA	NA	Cloudlock	PURCHASE OF CLOUDLOCK PLUGIN.	APRIGO	NA	SaaS	Private				3/28/2011	1 Year	$2,250.00	Yes	Melissa Benton	Brent Maravilla	Melissa Benton	EP11H000538

								FIPS 199 security category by type									
Department/Agency	IT Service Name	IT Application Name	Description of Service	Cloud Service Provider Name	Reseller (If Applicable)	Type (Iaas, SaaS, PaaS, Naas)	Cloud Service Model (Private, Public, Community, Hybrid)	C	I	A	Date Contract Initated	Contract Length (Base + Option Years)	Total Contract Value	Signed Service Level Agreement (SLA)	Contracting Officer's Representative	Contracting Officer	System Point of Contact	Contract Award ID
EPA			WEBCAMS& HEADSETS - CLOUD-BASED EMAIL AND COLLABORATION PILOT	CDW GOVERNMENT LLC							11/18/2011	1 Year	$5,747.40		Lin Darlington	Sharon Mason		EP12H000053
EPA	NA since these are computer peripheral devices	NA	WEBCAMS FOR THE CLOUD-BASED EMAIL PILOT PROJECT: MICROSOFT AND IBM PILOT PARTICIPANTS	CDW GOVERNMENT LLC	CDW Government LLC	NA	NA since product is hardware used to pilot other software	NA	NA	NA	2/23/2012	1 Year	$2,962.44	No (NA)	Dorothy Semazzi	Marisol Ventura	Dorothy Semazzi	EP12H000281
EPA	NA	Cloudlock	THIS IS A RENEWAL FOR CLOUDLOCK . OSIM 18-O-A33 SOFTWARE LICENSING.	CLOUDLOCK, INC	NA	SaaS	Private				4/17/2012	1 Year	$4,000.00	Yes	Melissa Benton	Lin Pinskey	Melissa Benton	EP12H000377

								FIPS 199 security category by type									
Department/Agency	IT Service Name	IT Application Name	Description of Service	Cloud Service Provider Name	Reseller (If Applicable)	Type (Iaas, SaaS, PaaS, Naas)	Cloud Service Model (Private, Public, Community, Hybrid)	C	I	A	Date Contract Initated	Contract Length (Base + Option Years)	Total Contract Value	Signed Service Level Agreement (SLA)	Contracting Officer's Representative	Contracting Officer	System Point of Contact	Contract Award ID
EPA	Red Hat Linux Server	N/A	GLNPO: RED HAT LINUX ENTERPRISE SERVER SOFTWARE FOR THE GLNPO EXTERNAL SLAKES NETWORK, TO SUPPORT THE GREAT LAKES OFFICE EXTERNAL PRIVATE CLOUD PAAS (PLATFORM AS A SERVICE). INCLUDES A 2 YEAR SERVICE AGREEMENT.	DLT SOLUTIONS, INC.	This procurement was a simple software purchase with maintenance agreement.						4/18/2012	2 Years	$5,757.95	No	John Piper	Donald Anderson		EPG12500097
EPA	WCF PCCLOUD	NA	NCC CLOUD HOSTING - CGI FEDERAL - CULLEN	CGI FEDERAL INCORPORATED	NONE	IAAS	Community	M	M	M	6/25/2012	3 Years	IDIQ	YES	Michael Cullen	Joel P. Smith		EPG12D00241

								FIPS 199 security category by type								
Department/Agency	IT Service Name	IT Application Name	Description of Service	Cloud Service Provider Name	Reseller (If Applicable)	Type (Iaas, SaaS, PaaS, Naas)	Cloud Service Model (Private, Public, Community, Hybrid)	C	I	A	Date Contract Initated	Contract Length (Base + Option Years)	Total Contract Value	Signed Service Level Agreement (SLA)	Contracting Officer's Representative	Contracting Officer	System Point of Contact	Contract Award ID
EPA	OPNet (now Riverbed) - THIS IS NOT OFFERED AS A SERVICE. Riverbed is a tool used to monitor/troubleshoot the OEI/OTOP/NCC application hosting environment.	Riverbed performance analysis system is used exclusively by NCC operations support contractors. Its capabilities are not available outside of the OEI/OTOP/NCC.	OPNET HARDWARE AND SOFTWARE WERE ACQUIRED TO ADD BADLY NEEDED APPLICATION PERFORMANCE MANAGEMENT (APM) CAPABILITIES TO THE NCC INFRASTRUCTURE. OPNET'S NICHE MARKET IS APM AND OFFERS MANY	OPNET TECHNOLOGIES, INC.	The OpNet performance analysis hardware and software was acquired directly through OpNet. Maintenance agreements for the hardware and software will now be acquired either directly through Riverbed or a reseller. OAM will determine the appropriate contract vehicle for maintenance renewal which is due on May 5, 2014.		not applicable since this is not a cloud service.	NA this is internal use only			6/6/2013	1 Year	$37,227.09	NA - this is internal use only	John B. Smith	John B. Smith		EP13D000222
EPA		N/A	SYMANTEC PROTECTION ENGINE FOR CLOUD SERVICES 7.0, ANNUAL RENEWAL	EDAPTIVE SYSTEMS, L.L.C.	This product is a third party software that scans attachments and content for malware and threat detection prior to document upload into the Office of Inspector General fabricated storage device. The word "Cloud" referenced in the product name is misleading.						1/29/2013	! Year	$1,165.00		Clara Cromer	Sherman Farves		EP13I000010

Joint Office of Administration and Resources Management and Office of Water Responses to Draft Report and OIG Comments (June 4, 2014)

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Audit Report No. OA-FY14-0126 "EPA Is Not Fully Aware of Its Use of Cloud Computing Technologies" dated July 7, 2014

FROM: Craig E. Hooks, Assistant Administrator
Office of Administration and Resources Management

Nancy Stoner, Acting Assistant Administrator
Office of Water

TO: Rudolph M. Brevard, Director
Information Resources Management Audits
Office of the Inspector General

Thank you for the opportunity to respond to the factual accuracy of the draft audit report "Office of Inspector General Draft Audit Report No. OA-FY14-0126 "EPA Is Not Fully Aware of Its Use of Cloud Computing Technologies" dated July 7, 2014.

The EPA agrees that the OIG's Council on the Inspectors General on Integrity and Efficiency Cloud Computing Collaboration Results Matrix is factually correct. However, throughout the fieldwork and data collection phase of the audit, the EPA was concerned with the OIG's narrow approach of evaluating EPA's use of cloud computing technologies.

The OIG requested that the Office of Administration and Resources Management provide data on EPA procurements for cloud computing but the draft audit focused on only one order under a Blanket Purchase Agreement. The audited BPA was established to procure technical support to develop, maintain, and revise the EPA's Electronic Notice of Intent and Permit Management Oversight Processing Systems, not to procure cloud services. As a result, the performance work statement solicited under the BPA did not contain a cloud services requirements and was not considered a cloud contract. However, in response to the solicitation, vendors proposed their best technical solutions for completing performance work statement tasks, and the awardee offered a technical solution that included the cloud, which was provided under a subcontract. Because of the afore-mentioned circumstances surrounding this procurement, the primary order did not contain cloud specific terms and conditions such as terms of service clauses and service level agreements.

In light of advances in cloud computing and the federal security management controls the Office of Water will evaluate its management controls to make sure our contracts are adhering to federal and EPA policies, procedures, and guidance with regards to cloud computing. Additionally, OARM acknowledges responsibility for ensuring contracts awarded also contain the appropriate terms and conditions, and clauses, applicable to the technical nature of the requirement. OARM had advised the OIG that the Federal Procurement Data System, the primary source of acquisition data government-wide, does not collect data specifically on cloud computing and therefore not be relied on for the questionnaire on this subject.

Please contact John Bashista, Director, Office of Acquisition Management, OARM, at 202-564-4310, or Lisa Maass, OAM Audit Follow-up Coordinator, OARM, at 202-564-2498 for acquisition related questions. For questions regarding the Office of Water, please contact Thomas Dabolt, Director, IM/IT Project Management Office, OW, at 202-564-1450, or Vince Allen, Assistant Information Management Officer, OW, at 202-564-1675.

Attachment

cc:
Charles Dade
Albert Schmidt
Nanci Gelb
John Showman
Thomas Dabolt
John Bashista
Marilyn Ramos
Vince Allen
Brandon McDowell
Lisa Maass

OIG Comments

During the entrance meeting, the OIG indicated that OAM should coordinate with the Office of Environmental Information (OEI) in determining the population of cloud IT services. The OIG did not identify any particular data system for OAM to use to identify the population of the EPA's cloud IT services. This would be something that the agency would need to identify and track as a part of its procurement process to ensure that appropriate clauses to protect the government are included during the procurement process. The OIG did not rely on any database when performing the audit work.

Prior to starting work on this audit, we were in the process of performing a cloud audit related to two of OEI's cloud initiatives. During that separate audit, we collected information that made us aware of two cloud initiatives within other program offices. Since we selected two cloud initiatives from OEI during the other audit, we selected one of the initiatives from a different program office to not overburden OEI. We selected the cloud initiative for testing as a part of this review prior to receiving the completed cloud survey from the agency.

Appendix C

Distribution

Office of the Administrator
Assistant Administrator for Administration and Resources Management
Assistant Administrator for Water
Assistant Administrator for Environmental Information and Chief Information Officer
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs and Environmental Education
Principal Deputy Assistant Administrator for Administration and Resources Management
Principal Deputy Assistant Administrator for Water
Principal Deputy Assistant Administrator for Environmental Information
Audit Follow-Up Coordinator, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of Water