U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System

Report No. 15-P-0295 **September 24, 2015**

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

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Albert Schmidt

Abbreviations

CFR	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CSP	Cloud Service Provider
EPA	U.S. Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FOIA	Freedom of Information Act
ICIS	Integrated Compliance Information System
IT	Information Technology
NIST	National Institute of Standards and Technology
OAM	Office of Acquisition Management
OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
OW	Office of Water
PMOS	Permit Management Oversight System

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

15-P-0295
September 24, 2015

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 the adoption of cloud computing for the Office of Water's Permit Management Oversight System (PMOS). We also reviewed an executed contract between the agency and a cloud service provider for compliance with applicable standards.

The PMOS is a Web-based application developed to meet the needs of the Office of Wastewater Management within the Office of Water. PMOS enables tracking and managing of the Priority Permit Initiative. PMOS enables EPA headquarters, EPA regions and individual states to work collaboratively to designate, track and report on the progress of priority permits.

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

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

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

The full report is at:
www.epa.gov/oig/reports/2015/20150924-15-P-0295.pdf

EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System

What We Found

Inadequate contract oversight jeopardized information security and government transparency.

The EPA is not fully aware of the extent of its use of cloud services, and thereby is missing an opportunity to help make the most efficient use of its limited resources regarding cloud-based acquisitions.

The Office of Water did not follow EPA procedures when implementing PMOS, and the office did not know whether it was in the agency's best interest to establish the system.

Additionally, inadequate oversight of the Office of Water's PMOS contractor resulted in inadequate controls over EPA data. In particular, the EPA failed to establish adequate requirements for the hosting of PMOS, resulting in PMOS being hosted in a cloud service provider's environment that did not comply with federal security requirements. There was also no assurance that the EPA has access to the service provider's cloud environment for audit and investigative purposes. In addition, the service provider's terms of service were not compliant with the Federal Risk and Authorization Management Program.

Furthermore, the PMOS jeopardized government transparency by being hosted on an Internet domain registered to a prior contractor, and by allowing the service provider to host PMOS-provided email services that may not be considered when responding to Freedom of Information Act requests.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Water, the Assistant Administrator for Administration and Resources Management, and the Chief Information Officer undertake seven corrective actions to address deficiencies in the EPA's cloud computing initiatives. Among other things, we recommend that the EPA take steps to appoint a lead office to evaluate information technology hosting proposals, develop a cloud system inventory, and develop guidance and train personnel on how to identify vendor proposals that may include cloud services. We also recommend that EPA take steps to develop and implement an approved PMOS system authorization package, determine the cost effectiveness for operating PMOS, and search the PMOS hosting environment for potential EPA records.

While the EPA agreed with our recommendations, management provided corrective actions and completion dates that only satisfied four of the recommendations. The agency did not provide sufficient information to allow us to determine whether its intended corrective actions would address our concerns for the three remaining recommendations. These three recommendations are considered unresolved pending the agency's response to the final report.

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

THE INSPECTOR GENERAL

September 24, 2015

MEMORANDUM

SUBJECT: Report: EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System
Report No. 15-P-0295

FROM: Arthur A. Elkins Jr.

TO: Ken Kopocis, Deputy Assistant Administrator
Office of Water

Karl Brooks, Acting Assistant Administrator
Office of Administration and Resources Management

Ann Dunkin, Chief Information Officer
Office of Environmental Information

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The EPA offices responsible for implementing the recommendations are the Office of Water, the Office of Administration and Resources Management, and the Office of Environmental Information.

Action Required

The Office of Water did not provide sufficient information to allow us to determine whether its intended corrective actions address three of the recommendations. These recommendations will remain unresolved until the office provides planned corrective actions in response to the final report. The Office of Environmental Information and the Office of Administration and Resources Management provided agreed-to corrective actions and planned completion dates. Therefore, no further response is required by these offices.

In accordance with EPA Manual 2750, the Office of Water is required to provide a written response to this report within 60 calendar days. The office should include planned corrective actions and completion dates for all unresolved recommendations. The response will be posted on the OIG's public website, along with our memorandum commenting on the response. The response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation

Act of 1973, as amended. The final response should not contain data that should not be released to the public; if the response contains such data, the office should identify the data for redaction or removal along with corresponding justification.

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

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to evaluate the adoption of cloud computing for the Office of Water's (OW's) Permit Management Oversight System (PMOS), and to review an executed contract between the agency and a cloud service provider for compliance with applicable standards.

Background

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed a survey and asked its members to contact their respective agencies and collect information about the deployment of cloud computing technologies. We published the test results to answer the survey questions in EPA OIG Report No. 14-P-0323, *EPA Is Not Fully Aware of the Extent of Its Use of Cloud Computing Technologies*, issued July 24, 2014. The EPA OIG selected OW's current PMOS contract for testing. While completing the CIGIE survey questions, we collected and reviewed information regarding the hosting of PMOS.

The December 8, 2011, Office of Management and Budget (OMB) "Memorandum for Chief Information Officers: Security Authorization of Information Systems in Cloud Computing Environments" provides guidelines for the development of the Federal Risk and Authorization Management Program (FedRAMP). The goal of FedRAMP was to provide a cost-effective, risk-based approach for executive departments and agencies to procure cloud services. FedRAMP was to make available multiple items, including:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels.

- Standardized contract language to help executive departments and agencies integrate FedRAMP requirements and best practices into acquisition.

On February 24, 2012, the federal Chief Information Officer (CIO) Council, and the Chief Acquisition Officers Council, in coordination with the Federal Cloud Compliance Committee, published *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*. This publication highlighted unique requirements for agencies to use when implementing cloud computing contracts.

In October 2012, OW used the Office of Administration and Resources Management's (OARM's) Office of Acquisition Management (OAM) to contract for a vendor to maintain and host the PMOS application. PMOS was hosted by a service provider whose hosting environment had cloud characteristics.

The service provider's hosting environment 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*. NIST defines cloud computing as:

> … a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

PMOS is a Web-based application designed to meet the management needs of OW's Office of Wastewater Management. PMOS enabled tracking and managing the Priority Permit Initiative, which is a key budget measure of the EPA's surface water performance. PMOS enabled EPA headquarters, EPA regions and individual states to work collaboratively to designate, track and report on the progress of priority permits.

Responsible Offices

OW owns the PMOS application and data. OW is responsible for implementing the Clean Water Act and the Safe Drinking Water Act. The Clean Water Act authorizes the National Pollutant Discharge Elimination System permit program, which controls water pollution by regulating point sources that discharge pollutants into waters of the United States. OW's Office of Wastewater Management used the information within PMOS to report the performance of the National Pollutant Discharge Elimination System program to OMB as a measure under the Government Performance and Results Act. OW is responsible for appointing a Contracting Officer's Representative who assists in the technical monitoring and administration of the PMOS contract.

The Contracting Officer within OAM was responsible for planning, awarding and administering the PMOS contract. OAM is also responsible for issuing and interpreting acquisition regulations, administering training for contracting and program acquisition personnel, providing advice and oversight to regional procurement offices, and providing information technology (IT) improvements for acquisition.

The Office of Environmental Information's (OEI's) Office of Technology Operations and Planning is responsible for IT investment management, and the development of policies and standards to guide IT expenditures and operations.

Scope and Methodology

We performed the audit work related to completing the CIGIE matrix from January 2014 through July 2015 at EPA headquarters in Washington, D.C. We performed this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine compliance with key standards identified in a CIGIE questionnaire, we limited the review to PMOS, and to a contract executed between the agency and a cloud service provider. We did not perform a detailed review of the associated contract. We interviewed and collected documentation from OAM and OW management and staff responsible for planning, procuring, maintaining and monitoring the PMOS contract.

Prior Audit Reports

Prior to this report, we issued two audit reports related to cloud computing efforts at the EPA.

EPA OIG Report No. 14-P-0332, *Cloud Oversight Resulted in Unsubstantiated and Missed Opportunities for Savings, Unused and Undelivered Services, and Incomplete Policies*, issued August 15, 2014, noted that although the EPA developed processes to monitor cloud vendors, those controls were incomplete and needed improvement. That report contained 11 recommendations that the agency agreed to implement. We obtained the status of those recommendations by collecting information on agency corrective actions and data the EPA recorded in its Management Audit Tracking System. The agency reported that it had completed corrective actions for Recommendations 2, 3 and 7. The agency is planning to complete corrective actions for the remaining eight recommendations by November 2017.

As part of a CIGIE survey, we collected information on EPA efforts to adopt cloud computing technologies. We reported that information in EPA OIG Report No. 14-P-0323, *EPA Is Not Fully Aware of the Extent of Its Use of Cloud Computing Technologies*, issued July 24, 2014. That report did not contain any recommendations.

Chapter 2
Incomplete and Inaccurate Inventory of Cloud Services Contributed to PMOS Oversight Concerns

The EPA's lack of awareness of the extent of its use of cloud services contributed to our concerns regarding PMOS oversight. OMB requires agencies to report on cloud initiatives. However, OEI did not provide internal guidance for EPA regions and program offices to use in identifying cloud initiatives. Without an accurate and complete cloud system inventory, for systems such as PMOS and other cloud services, the EPA cannot ensure that appropriate language is included in contracts or that adequate controls are in place to protect the agency's systems and data.

EPA Did Not Maintain a Complete and Accurate Inventory

The EPA could not readily or easily identify and report on IT systems that use cloud services. When developing a listing of contracts for cloud services, OAM indicated that the listing was completed by performing a search for the word "cloud" in the procurement description. As a result, regardless of whether a contract was a cloud contract, the contract would only be included on the list if the word "cloud" appeared in the description of the procurement. Although we did not perform a complete review of the cloud inventory returned by OAM, the following issues were identified with the inventory provided:

- One application was incorrectly listed as a cloud application.
- Two additional applications that appeared to be cloud applications were not included in the survey results – in particularly, one system being PMOS which was selected for detailed testing during this audit.

The publication *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*[1] states:

> Before signing a cloud computing contract, a Federal agency should take care to understand the CSP [cloud service provider] environment and where Federal data might reside.

According to OMB Circular A-123, *Management's Responsibility for Internal Control*, Chapter I "Management is responsible for developing and maintaining effective internal control." As a result, prior to entering into a contract the EPA should determine whether the contract is for a cloud service, to ensure that adequate controls are implemented. Further, OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, Sections 55.5 and 55.6,

[1] A joint publication of the CIO Council and the Chief Acquisition Officers Council.

requires the EPA to submit an "Agency Cloud Spending Summary," which includes providing IT investment budget information for cloud computing deployment and service models. Cloud computing deployment and service models are provided in NIST Special Publication 800-145, *Definition of Cloud Computing*.

An OAM representative said the office has no database that specifically identifies "cloud" procurements. The EPA does not have an office or a group that centrally manages cloud service contracts. The management and procurement of contracts (including cloud services) is shared between OAM and the program offices or regions. Although OAM may not maintain a database of cloud applications, there could be other applications or databases within the EPA that may be used to identify applications residing in a cloud. Examples of EPA applications that may be used include:

- **OEI's Registry of EPA Applications, Models and Databases.** This registry is the authoritative source of information about the EPA's applications, systems and models.

- **OARM's EPA Acquisition System.** The system is a centralized system for all EPA product and service acquisitions. The system enables all key stakeholders in the procurement process to use one automated system throughout the acquisition life cycle—from requisitioning to contract closeout.

Furthermore, OEI has not issued procedures instructing the agency how to identify cloud initiatives. Without this guidance, there is no assurance that the EPA will be providing OMB with a correct "Agency Cloud Spending Summary."

Deficiencies in EPA policies and procedures relative to cloud computing were previously reported in Chapter 1 of EPA OIG Report No. 14-P-0332. In response to Recommendation 11 from that prior report, OEI agreed to publish detailed instructions for agency programs to use when they consider moving applications to the cloud, including instructions that fully address federal guidance. OEI said the instructions would be published March 31, 2016.

In addition, on March 23, 2015, the EPA's CIO sent an email to all of the agency's Information Management Officers stating that all IT procurements over $10,000 need to be approved by the CIO. The email used the IT definition obtained from OMB Circular A-130, *Management of Federal Resources*. The email, however, did not require requests for purchases to include instructions for vendors to provide information that can be evaluated to determine whether IT or cloud services are included in the procurement. This lack of information directly contributed to the EPA not questioning its contractors in order to gain an understanding how the vendor planned to host the PMOS application. As a result, the agency may not properly recognize a contract as a cloud service, which could lead to unrecognized cloud services that are not FedRAMP compliant. Without a complete inventory of cloud services, the EPA lacks a valuable resource that would help the agency make the most efficient use of its limited resources.

Conclusion

The EPA was not fully aware of the extent of its use of cloud services, and thereby was missing an opportunity to help make the most efficient use of its limited resources regarding cloud-based acquisitions.

Recommendations

We recommend that the Chief Information Officer:

1. Appoint the National Computing Center as the agency lead for evaluating all IT hosting proposals to determine if the hosting is cost beneficial and meets federal requirements.

2. Develop guidance for OARM and program offices to identify IT procurements, so that IT and cloud procurements can be identified; and develop and implement an oversight to validate the guidance is being followed.

3. Develop and maintain an inventory of cloud systems.

Agency Response to Draft Report and OIG Evaluation

We received responses to the draft report from OEI and OARM. Based on OEI and OARM responses, we made changes as needed. In response to the draft report's Recommendation 1, OEI provided two corrective actions to address our concerns. Based on subsequent meetings with OEI, we agreed with OEI's alternative corrective actions. As a result, we revised our recommendations, and OEI agreed with our revised recommendations. We believe Recommendations 1 and 2 fully address our concerns, and we consider these recommendations open with agreed-to corrective actions pending.

EPA management agreed that OEI would assume responsibility for Recommendation 3, and OEI provided a planned date to complete the corrective action. We consider this recommendation open with the agreed-to corrective action pending.

Appendix B contains OARM's response, and Appendix A contains OEI's response.

Chapter 3
PMOS Implementation Did Not Follow OMB Guidance

OW did not perform a cost-benefit analysis to determine whether it was in the EPA's best interest to develop PMOS, and OW did not have a security plan or risk assessment for PMOS. OMB also provides guidance for completing cost-benefit analyses. OMB guidance provides that security plans are required for all systems, and that the risk assessment approach should be used to determine adequate security.

OW had concerns about using a preexisting permit application instead of developing PMOS. Also, the security plan was not developed, and the risk assessment was not performed because OW only considered PMOS a "prototype," even though PMOS was used in production. As a result, the EPA did not know whether it was cost beneficial to use the PMOS application, or whether the information in PMOS was secure.

No Cost-Benefit Analysis Was Performed on PMOS

EPA purchased PMOS without performing a cost-benefit analysis. PMOS was purchased even though the EPA's Office of Enforcement and Compliance Assurance already had the Integrated Compliance Information System (ICIS), and OW had indicated ICIS may have the ability to track the same information being tracked in PMOS.

OMB Circular A-130, Revised, Section 8.a.a(e), says agencies will "[i]ntegrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition and use of information technology." In addition, according to OMB Circular No. A-94, Revised, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Section 5, "Benefit-cost analysis is recommended as the technique to use in a formal economic analysis of government programs or projects."

OW representatives expressed some concerns regarding ICIS use. Specifically, representatives said the following:

- Major changes would be required to allow ICIS to handle some of the transactional components (e.g., adding, checking status, and other priority permits tracking work flow) necessary to track priority permits. In the future, it is envisioned that ICIS will be capable of handling the transactions and the priority permits program.

- The General Permit Inventory (i.e., number and type) could not be accurately counted, because ICIS did not become fully operational for all states until 2012. OW representatives further noted that New Jersey still does not report to ICIS.

- ICIS does not collect all necessary information. Specifically, states delegated National Pollutant Discharge Elimination System authority have only committed to report elements from the Permit Compliance System Policy Statement.

OW cited concerns with using ICIS to perform the same function as PMOS; however, a formal documented cost-benefit analysis was not performed to determine whether it was more cost beneficial to do one of the following:

- Use the stand-alone PMOS application.
- Make the necessary adjustments to ICIS to include the same functionality as PMOS.
- Develop a comprehensive application to replace ICIS and similar applications associated with permitting used within the EPA.

As a result, the EPA did not know whether it was in the agency's best interest to purchase the PMOS application.

PMOS Did Not Have a Security Plan or Risk Assessment

OW did not have a security plan, risk assessment or associated authorization to operate the PMOS application. OMB Circular A-130, Appendix III, Section B.a.2, states "all systems require security plans." Furthermore, this appendix states that determining:

> … adequate security will require that a risk-based approach be used. This risk-assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and effectiveness of current or proposed safeguards.

NIST Special Publication 800-30, Revision 1, provides guidance for conducting risk assessments, and NIST Special Publication 800-18, Revision 1, provides guidance for developing security plans.

In addition, the EPA's System Life Cycle Management procedure, CIO 2121-P-03.0, Section 6.3, indicates that a "Security Risk Assessment" needs to be conducted in the definition phase of the System Life Cycle Management process and be updated in the acquisition and development phase of the product for both major and non-major systems. Since the Security Risk Assessment did not exist for the PMOS application, the agency's System Life Cycle Management procedure was not followed.

The agency's System Life Cycle Management indicates that during the acquisition and development phase, an Authorization to Operate a system must be obtained from a senior EPA official. Also, the EPA's Information Security Interim Planning Procedures, CIO-2150.3-P-12.1, indicate that the baseline risk assessment and security plans are deliverables requiring development during system planning.

As a result, questions remain as to whether the PMOS application ever complied with required security standards. There are also questions about whether management accepted unknown risks operating a system that had not gone through a structured security planning process to mitigate risks to an acceptable level. Furthermore, management cannot be assured that the integrity of the data processed by the PMOS application was suitable for its intended purpose.

Conclusion

The EPA did not know whether it was cost beneficial to use the PMOS application, since OW did not perform a cost-benefit analysis to determine whether it was in the EPA's best interest to develop PMOS. Additionally, the data integrity of the PMOS application was at risk, because EPA officials did not make risk-based decisions regarding how to best protect the system from threats.

Recommendations

We recommend that the Assistant Administrator for Water:

4. Develop and implement an approved system authorization package (i.e., a risk assessment, System Security Plan, and Authorization to Operate), and perform annual security assessments for the PMOS application.

5. Perform a formal documented analysis to determine whether it would be more cost beneficial to either continue using PMOS; update ICIS to support the functions of the PMOS application; or develop a comprehensive application to replace PMOS, ICIS and similar applications associated with permitting used within the EPA.

Agency Response to Draft Report and OIG Evaluation

OW concurred with our recommendations. However, OW's response only addressed portions of the recommendation. OW did provide an authorization to operate for PMOS, but OW did not provide us with all the necessary documents needed for a complete system authorization package. Specifically, OW needs to provide the required security documentation for the PMOS application, because the controls inherited from the National Computing Center's General Support System are not defined at the application level.

OW cites the use of an application security certification form and security controls reportedly implemented by the PMOS hosting organization as the basis for OW's security authorization package. EPA guidance requires the system owner to develop a security authorization package consistent with NIST and ensure relied upon security controls are implemented and operating effectively. Therefore, we consider Recommendation 4 unresolved.

OW cites OMB and EPA guidance as the basis for not completing a cost-benefit analysis for the PMOS system. While the cost threshold for PMOS does not require a cost-benefit analysis, our audit disclosed that PMOS provides similar functionality as the EPA's ICIS, which is a major IT investment. Therefore, it is incumbent upon EPA management to make the most cost-effective use of funds when making IT investment decisions from a corporate perspective. Management should conduct a review of its IT investment portfolio and look for opportunities to save costs. We consider Recommendation 5 unresolved.

Appendix C contains the OW response.

Chapter 4
Vendor Monitoring Needs Improvement

PMOS was hosted in a service provider's hosting environment that did not meet federal requirements, and provided email services that may not be considered when responding to Freedom of Information Act (FOIA) requests. Additionally, neither the EPA, the prime contractor nor the cloud service provider owned the domain that hosted the PMOS application, thus limiting transparency. The conditions arose because the contracting officer was unaware that a prime contractor was using a cloud service provider to host the PMOS application and did not ensure the contract contained adequate controls to protect the government's interests. As a result, there was no assurance that the PMOS application was hosted in an environment that was in compliance with FedRAMP or FOIA.

PMOS Application Was Hosted in an Environment Not Compliant With Federal Regulations

The EPA did not establish the requirements for hosting the PMOS application within the Request for Proposal or in a subsequent contract for PMOS services. As a result, the new prime contractor responsible for supporting the system used a cloud service provider to host the PMOS application. That provider was not FedRAMP compliant, and the predefined terms and conditions of service for providing application hosting did not meet recommended federal requirements and best practices. Specifically, using CIGIE survey questions regarding the deployment of cloud computing technologies, our review disclosed weaknesses that include the following:

- The cloud service provider hosting the PMOS application was not FedRAMP compliant as required for cloud service providers hosting federal cloud services, per the December 8, 2011, OMB "Memorandum for Chief Information Officers: Security Authorization of Information Systems in Cloud Computing Environments."

- The EPA did not meet the best practices identified in *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*. For example, the terms and conditions of the service provider did not allow agencies to conduct forensic investigations for both criminal and non-criminal purposes without affecting data integrity and without interference from the cloud service provider. In addition, the terms and conditions did not require the cloud service provider to make only changes to the cloud environment under specific standard operating procedures agreed to by the cloud service provider and the EPA.

- The cloud service provider’s terms and conditions of service did not include a clause that allows the EPA access to the cloud service provider’s facilities, installations, technical capabilities, operations, documentation, records and databases to ensure privacy and security safeguards.

- The cloud service provider’s terms and conditions of service did not include a clause that would allow the EPA OIG access to examine any of the vendor’s records or interview any officer or employee regarding transactions pertaining to the agreed-to terms and conditions of service. This impeded the rights provided to the OIG under the Inspector General Act of 1978.

The December 8, 2011, OMB memorandum established federal policy for the protection of federal information in cloud services, defined agency responsibilities, and defined requirements for agencies using FedRAMP in the acquisition of cloud services. This policy, in part, required agencies to ensure acquisition requirements address maintaining FedRAMP security authorization requirements and that relevant contract provisions related to contractor reviews and inspections be included for cloud service providers.

Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service identified 10 areas requiring improved collaboration and alignment between agency program and procurement offices during the contract formation process. This publication states that:

> Before signing a cloud computing contract, a Federal agency should take care to understand the cloud service provider’s environment and where Federal data might reside. Some key things to consider include:
>
> - Ensure the contract clearly defines the specific requirements for data in motion and data at rest (including the location of data servers and redundant servers).
>
> - Fully incorporate the security controls as articulated in NIST Guidance in the agreement and understand how CSPs [cloud service providers] will implement those controls.
>
> - Contractually define a procedure for what CSPs must do in the event of any request for disclosure, subpoena, or other judicial process from outside the United States seeking access to agency data.

OAM indicated that the PMOS procurement order was for technical support services for an existing system, and the vendors were required to offer their best technical solution for completing the above tasks mentioned in the *Creating*

Effective Cloud Computing Contracts for the Federal Government publication. We brought to the EPA's attention that the PMOS system was being hosted by a cloud service provider, and OAM said it was not aware the prime contractor was using a cloud service provider. Additionally, the request for proposal did not specifically state how to perform the hosting service.

OAM is responsible for maintaining the *EPA Acquisition Guide* that contains the EPA's acquisition policies and procedures. However, these procedures provided no specific instructions on identifying cloud computing in procurements.

Since OAM did not understand that the prime contractor was using a cloud service to host PMOS, and the program office did not make OAM aware of the use of cloud services, OAM did not ensure that the contract contained terms and conditions specific to the performance of cloud services. As a result, the EPA placed the PMOS application into a computer environment without fully knowing the risks to the agency or whether the application was protected with appropriate security controls as required by federal guidance.

In response to the audit, OW moved the PMOS application into the EPA's domain and network.

Government Transparency Is Limited

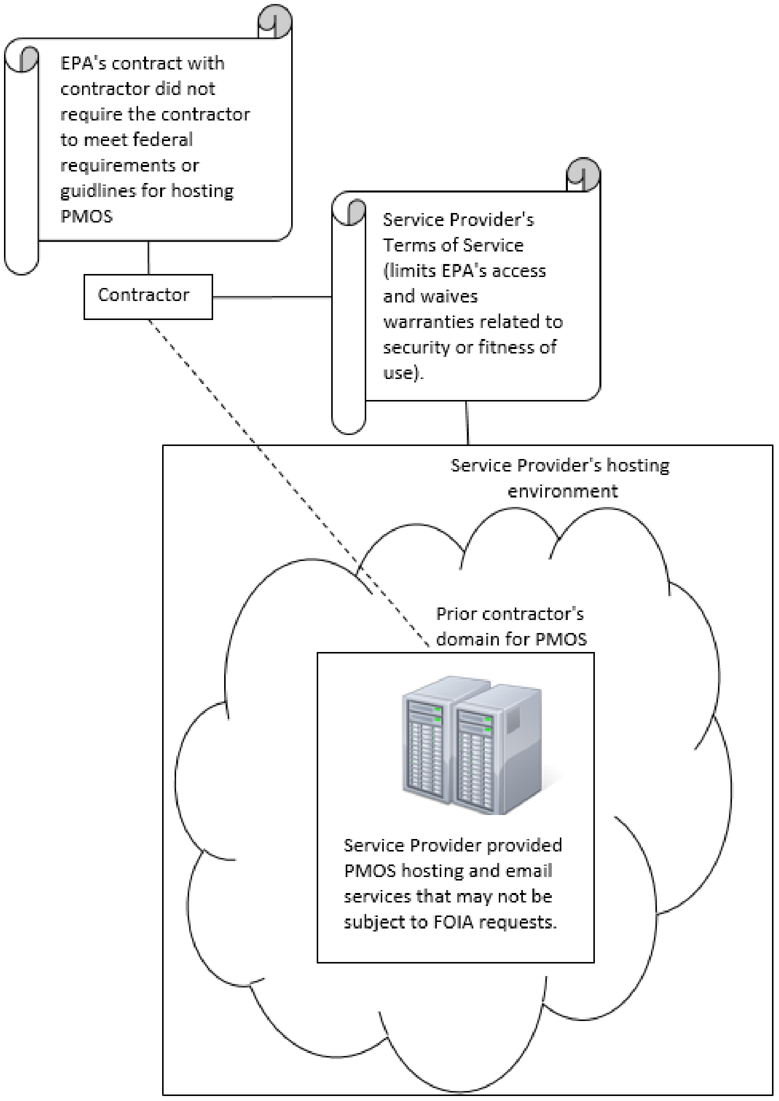
The PMOS Web application was hosted in an Internet domain (.com) owned by a prior PMOS contractor. The domain that hosted PMOS was not registered to the EPA or to the current contractor or service provider. Instead, the PMOS domain was registered to a prior contractor, which reduced the government's transparency. In addition, the prior contractor could have potentially caused other problems by:

- Redirecting traffic away from the PMOS server. Domain owners are able to define what Internet Protocol (IP) addresses to which a Uniform Resource Locator (URL) was assigned.

- Installing other Web servers unrelated to the EPA in the same domain. Since Web servers host websites and deliver pages to users upon demand, these Web servers could have hosted messages and websites that provided information that was not EPA supported.

Furthermore, the service provider provides email services as part of its hosting solution. Hosting email services within a domain established a method of communication that may not be considered for FOIA requests. Figure 1 provides a visual representation of the EPA's agreement with the contractor and the service provider prior to the PMOS application being moved into the agency's network.

Figure 1: Visual representation of the EPA's agreement with the contractor and service provider prior to August 29, 2014


EPA's contract with contractor did not require the contractor to meet federal requirements or guidlines for hosting PMOS
Contractor
Service Provider's Terms of Service (limits EPA's access and waives warranties related to security or fitness of use).
Service Provider's hosting environment
Prior contractor's domain for PMOS
Service Provider provided PMOS hosting and email services that may not be subject to FOIA requests.

EPA OIG Generated

OMB Memorandum M-10-06 states:

> The three principles of transparency, participation, and collaboration form the cornerstone of an open government. Transparency promotes accountability by providing the public with information about what the Government is doing. Participation allows members of the public to contribute ideas and expertise so that their government can make policies with the benefit of information that is widely dispersed in society. Collaboration improves the effectiveness of Government by encouraging partnerships and cooperation within the Federal Government, across levels of government, and between the Government and private institutions.

The Code of Federal Regulations (CFR), in 36 CFR Chapter XII – National Archives and Records Administration, Section 1236.22(b), states:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.

The EPA also developed a Records Management Policy, CIO 2155.3, that established specific requirements to effectively and efficiently identify, manage, search, retrieve and provide access to records throughout their lifecycle.

In addition, the contracting officer indicated that the agency was unaware that a service provider was providing hosting services until the OIG made inquiries about the hosting of the PMOS application. Not having the domain registered to EPA could result in:

- Users believing that the prior contractor is a current EPA contractor.
- The prior contractor using the PMOS domain for non-EPA business (which may redirect PMOS users to a non-EPA system).

Furthermore, since the service provider included email services as part of the hosting package, the capability existed for emails that were sent and received to not be considered when responding to FOIA requests. Although agency personnel indicated they were unaware the email capabilities existed, the existence of these capabilities could create concern the EPA may be circumventing federal records management requirements.

Conclusion

The EPA failed to establish adequate requirements for hosting the PMOS application. As a result, there was no assurance that the PMOS application was hosted in a secure environment or that FOIA was not being circumvented. This occurred because 1) the service provider hosting PMOS did not meet federal requirements and included email services that might not be considered when responding to FOIA requests; and 2) the EPA did not own the domain hosting the PMOS application, thereby reducing government transparency.

Recommendations

We recommend that the Assistant Administrator for Administration and Resources Management:

6. Update the *EPA Acquisition Guide* to require:

    a. Contracting Officers and Contracting Officer's Representatives to take training for recognizing the procurement of cloud services or other IT services.

    b. The procurement requestor to notify Contracting Officers when procurements may include cloud services or other IT services, so it can be determined if the CIO approved IT procurements over $10,000 and that appropriate clauses can be added to the contract.

We recommend that the Assistant Administrator for Water:

7. Perform and document a review to determine if the service provider's email services were used. Move any emails that would be subject to FOIA requests or preserved in accordance with the EPA's Records Management Policy.

Agency Response to Draft Report and OIG Evaluation

OARM and OW concurred with our recommendations. However, neither OARM nor OW provided sufficient information to allow us to determine whether their intended actions would satisfy the intent of our recommendations.

After we asked OARM about its response, OARM further clarified its response by providing support for the CIO approving IT procurements over $10,000, and for adding appropriate clauses to contracts. We consider Recommendation 6 closed and all agreed-to actions completed.

OW indicated that all emails pertaining to questions about PMOS or other communication were through the EPA contractor or the agency's mail system. Our audit disclosed that the PMOS hosting environment included email services. Email generated from the hosting platform's email system would be separate from the contract administration emails discussed in OW's response. During our audit, management did not provide evidence that no email existed within the PMOS hosting environment. Therefore, it is incumbent upon management to perform due diligence and obtain written verification as to whether the email services were used.

Additionally, if it is determined that the email services were used, OW needs to conduct a search for and preserve any potential records to ensure the EPA is compliant with FOIA requirements and the EPA's Records Management Policy. Recommendation 7 remains unresolved.

Appendix B contains OARM's response to the draft report, and Appendix C contains OW's response.

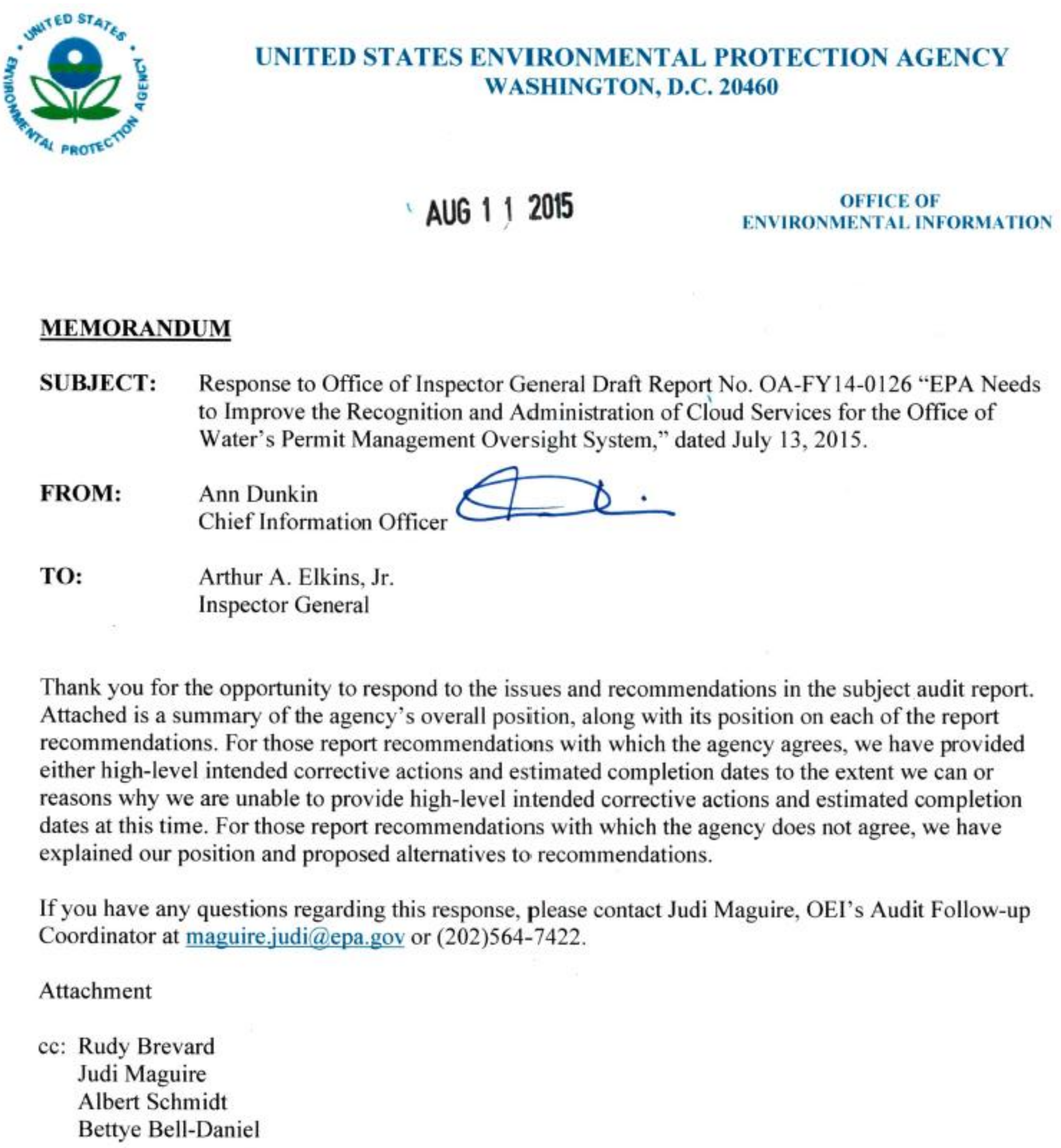
Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
1	6	Appoint the National Computing Center as the agency lead for evaluating all IT hosting proposals to determine if the hosting is cost beneficial and meets federal requirements.	O	Chief Information Officer	12/31/2015		
2	6	Develop guidance for OARM and program offices to identify IT procurements, so that IT and cloud procurements can be identified; and develop and implement an oversight to validate the guidance is being followed.	O	Chief Information Officer	12/11/2015		
3	6	Develop and maintain an inventory of cloud systems.	O	Chief Information Officer	3/31/2016		
4	9	Develop and implement an approved system authorization package (i.e., a risk assessment, System Security Plan, and Authorization to Operate), and perform annual security assessments for the PMOS application.	U	Assistant Administrator for Water			
5	9	Perform a formal documented analysis to determine whether it would be more cost beneficial to either continue using PMOS; update ICIS to support the functions of the PMOS application; or develop a comprehensive application to replace PMOS, ICIS and similar applications associated with permitting used within the EPA.	U	Assistant Administrator for Water			
6	16	Update the *EPA Acquisition Guide* to require: a. Contracting Officers and Contracting Officer's Representatives to take training for recognizing the procurement of cloud services or other IT services. b. The procurement requestor to notify Contracting Officers when procurements may include cloud services or other IT services, so it can be determined if the CIO approved IT procurements over $10,000 and that appropriate clauses can be added to the contract.	C	Assistant Administrator for Administration and Resources Management	8/14/2015		
7	16	Perform and document a review to determine if the service provider's email services were used. Move any emails that would be subject to FOIA requests or preserved in accordance with the EPA's Records Management Policy.	U	Assistant Administrator for Water			

[1] O = Recommendation is open with agreed-to corrective actions pending.
C = Recommendation is closed with all agreed-to actions completed.
U = Recommendation is unresolved with resolution efforts in progress.

Appendix A

OEI Response to Draft Report



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

AUG 11 2015

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY14-0126 "EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System," dated July 13, 2015.

FROM: Ann Dunkin
Chief Information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Attached is a summary of the agency's overall position, along with its position on each of the report recommendations. For those report recommendations with which the agency agrees, we have provided either high-level intended corrective actions and estimated completion dates to the extent we can or reasons why we are unable to provide high-level intended corrective actions and estimated completion dates at this time. For those report recommendations with which the agency does not agree, we have explained our position and proposed alternatives to recommendations.

If you have any questions regarding this response, please contact Judi Maguire, OEI's Audit Follow-up Coordinator at maguire.judi@epa.gov or (202)564-7422.

Attachment

cc: Rudy Brevard
Judi Maguire
Albert Schmidt
Bettye Bell-Daniel

OIG Recommendation
Recommendation 1: Provide guidance necessary to require requests for purchases to include instructions for vendors to provide information that can be evaluated to determine whether IT or cloud services are included in the procurement.

OEI Response:
As part of FITARA implementation, OEI has established the National Computing Center as our cloud services brokerage. NCC will, in consultation with agency stakeholders, assist in the evaluation of hosting locations for each new acquisition, re-competition or refresh of IT systems/applications. This evaluation will be accomplished through a standard process that will yield the essential documentation needed to perform and "apples-to-apples" comparison and determine the optimal hosting location for the application/system. Resulting documentation will be used to inform stakeholders and support FITARA recommendations/decisions. This will allow OEI to establish both the type and provider for application hosting for all EPA applications going forward.

NCC plans to have it's the first phase of its cloud brokerage services available to the EPA as a whole by the end of calendar year 2015. This phase includes:

i. EPA Private Cloud ready to support partially automated self-service
ii. Third party Cloud Service Provides (CSP) in place
iii. Templates for cost effectiveness comparisons
[NOTE – It should also be clarified that NCC does not make the ultimate hosting decision, but provides the relevant data. The CIO, as part of the FITARA process, will make the final decision.]

Due Date - 12/31/15

In addition, as part of the FITARA implementation process OEI is currently working with OAM to create guidance for determining when an acquisition has an IT component.

As indicated above, we are working with OARM on an ongoing basis on this question, and it is not addressed in the interim guidance. We will include it in the final guidance. A key dependency in this action is receiving OMB approval of our FITARA Implementation Plan. This was submitted on August 15, 2015. OMB has indicated that it will complete its feedback by the end of calendar year 2015. We recommend the following milestone:

- Within 30 days of receiving OMB comment/approval on EPA's FITARA Implementation Plan, the CIO will issue a memo to the CAO with guidance on how OARM should identify planned acquisitions that have an IT element.

- If OMB has not issued approval/comment on EPA's FITARA Implementation Plan by November 30, 2015, the CIO should issue a memo to the CAO with interim guidance on how OARM should identify planned acquisitions that have an IT element, and issue a follow-up memorandum, if necessary, after OMB feedback.

Due Date – 12/11/15

OIG Recommendation
Recommendation 2: Develop and maintain an inventory of cloud systems.

OEI Response: OEI agrees with the IG that READ is an appropriate location to identify the type of hosting for each application rather than establishing yet another database. A hosting type field does not currently exist in READ, but OEI will add a data element to READ whereby the owner of a system will identify the type of hosting for a system.

Estimated Date of Completion **3/31/2016**

Appendix B

OARM Response to Draft Report

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

AUG 19 2015

OFFICE OF
ADMINISTRATION
AND RESOURCES
MANAGEMENT

MEMORANDUM

SUBJECT: Response to OIG Draft Audit Report OA-FY14-0126 "EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System" dated July 13, 2015

FROM: Karl Brooks, Acting Assistant Administrator

TO: Rudolph M. Brevard, Director
Information Resources Management Audits

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. Attached is a summary of OARM's position on applicable report recommendations. In the attached, we have provided corrective actions and completion dates for those actions.

If you have any questions regarding this response, please contact Lisa M. Maass, OAM Audit Follow-Up Coordinator, at (202) 564-2498.

Attachments

cc: Donna Vizian
John Showman
John Bashista
Lisa Maass

Subj: OIG Draft Audit OA-FY14-0126 "EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System

Audit Recommendation

3. Develop and maintain an inventory of cloud systems.

OARM Response

OARM proposes an alternate corrective action to audit recommendation 2. Accordingly, OEI agrees that the Registry of EPA Applications, Models, and Databases is an appropriate location to identify and host cloud systems, and is verifying and identifying a hosting field in which to collect and store such data in same. Based upon the above-described response, the EPA office responsible for this corrective action is OEI.

OEI Completion Date: TBD by OEI

5. Update the EPA Acquisition Guide to require:

- **a. Contracting Officers and Contracting Officers Representatives to take training for recognizing the procurement of cloud services or other IT services.**
- **b. The procurement requestor to notify the Contracting Officers when procurements may include cloud service or other IT services, so it can be determined if the CIO approved IT procurements over $10,000 and that appropriate clauses can be added to the contract.**

OARM agrees with this recommendation. Under attached IPN 15-07 "Approval of Information Technology Acquisitions", the "Policy" Section states:
"(a) Effective immediately, approval for all IT product and service acquisitions shall be obtained from the CIO or delegated representative of the CIO. Approvals shall be obtained using the FITARA Approval Process found at: http//oamintra.epa.gov/it approval. This approval process is subject to change and requiring officials should continually check back for updates to the process.
(b) The requiring official, typically the Contracting Officer's Representative (COR), is responsible for submitting the request and obtaining approval for an IT acquisition. After approval is received, a copy of the approval shall be included with the Advanced Procurement Plan (APP), if an APP is required in accordance with EPAAG 7.1.1. If an APP is not required, a copy of the approval shall be included with the requisition.
(c) Requiring officials should work with their SIO and/or IMO to determine if their requirements are subject to this policy, to decide from which individual(s) approval is needed, and to answer questions to resolve any issues from the approver(s).
(d) The Contracting Officer (CO) shall review the APP or requisition as appropriate for each IT acquisition to ensure the proper approval was obtained in accordance with this section. The CO shall not solicit or award a contract, order, or work assignment for IT products or services without verifying the necessary approval was obtained. The CO will include a copy of the approval in the contract file."

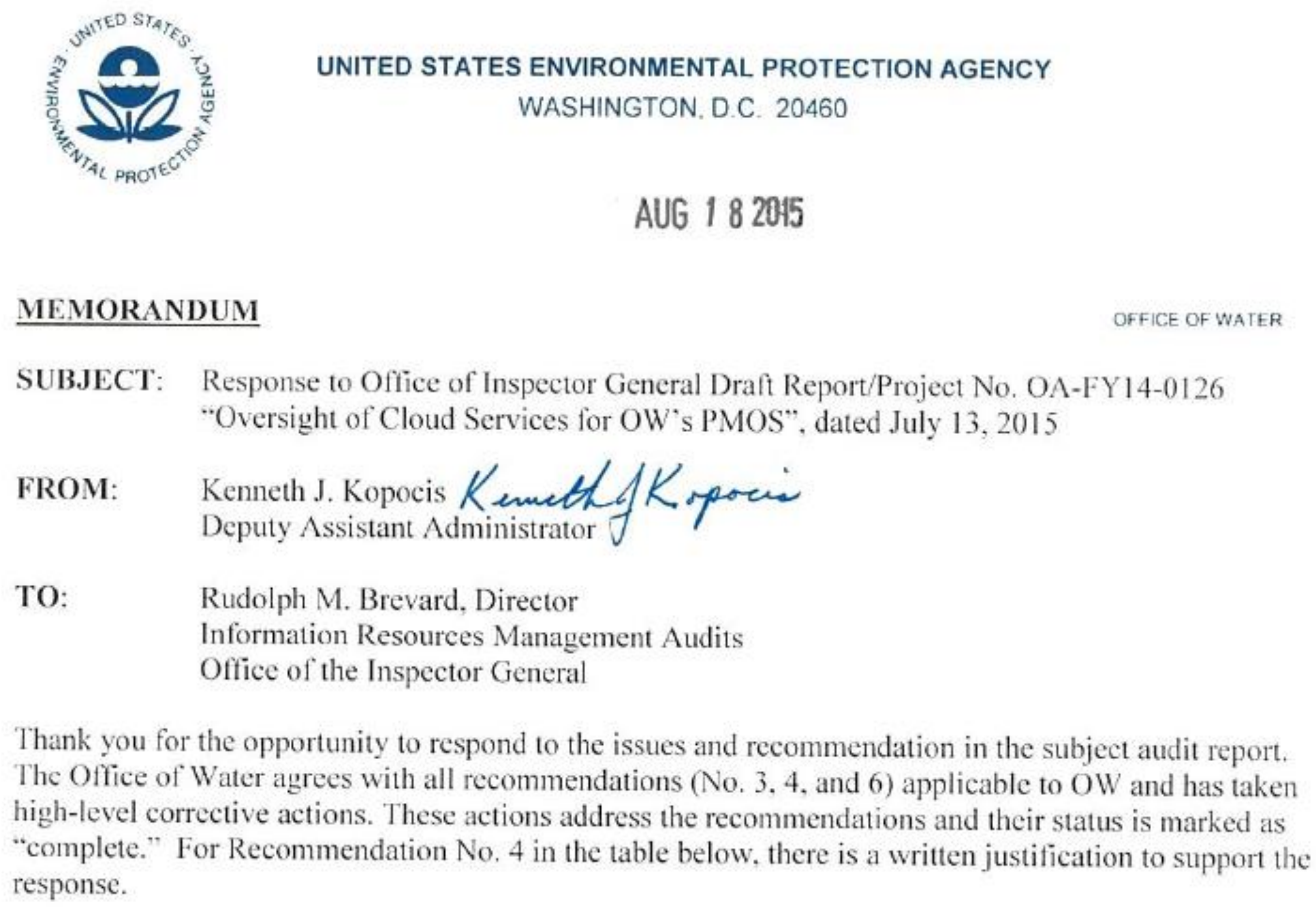
Regarding recommendation 5.a, while the EPA has no current plans to train COs and CORs on recognizing cloud procurements, through the above-described process COs and CORs will understand the IT supplies/services being procured in order to ensure appropriate clauses, and other terms and conditions, are included in the resulting contract.

Regarding recommendation 5.b, again through the above-described process, COs and CORs will understand the IT supplies/services being procured in order to ensure appropriate clauses, and other terms and conditions, are included in the resulting contract.

OARM Completion Date: August 4, 2015

Appendix C

OW Response to Draft Report



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

AUG 18 2015

MEMORANDUM

OFFICE OF WATER

SUBJECT: Response to Office of Inspector General Draft Report/Project No. OA-FY14-0126 "Oversight of Cloud Services for OW's PMOS", dated July 13, 2015

FROM: Kenneth J. Kopocis Kenneth J Kopocis
Deputy Assistant Administrator

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

Thank you for the opportunity to respond to the issues and recommendation in the subject audit report. The Office of Water agrees with all recommendations (No. 3, 4, and 6) applicable to OW and has taken high-level corrective actions. These actions address the recommendations and their status is marked as "complete." For Recommendation No. 4 in the table below, there is a written justification to support the response.

AGENCY'S RESPONSE TO REPORT RECOMMENDATIONS

Recommendation 3: Develop and implement an approved system authorization package (i.e., a risk assessment, System Security Plan, and Authorization to Operate), and perform annual security assessments for the PMOS application.

OW Response: PMOS was moved to the EPA's National Computer Center (NCC) on 8/29/2014, a Federally managed hosting facility. The Agency Application Security Certification (ASC) form was used as the authorization package based on the systems FIPS 199 categorization of low. The NCC environment where PMOS resides today is covered by a FIPS 199 moderate hosting environment inheriting all NCC General Support System (GSS) controls defined by NIST SP 800-53 Rev.4.

Estimated Completion Date: 8/29/2014

Recommendation 4: Perform a formal documented analysis to determine whether it would be more cost beneficial to either continue using PMOS; update ICIS to support the functions of the

PMOS application; or develop a comprehensive application to replace PMOS, ICIS and similar applications associated with permitting used within the EPA.

OW Response: Existing OMB eCPIC and Agency CIO SLCM reporting requirements, and internal OW IM/IT policy and procedures do not require a formal IT Alternatives Analysis to be produced unless the investment is classified as a CPIC Lite expenditure exceeding 250k annually. A written justification (approved by OW's IMO) that outlines the business case is also available and is attached.

Estimated Completion Date: 8/14/2015.

Recommendation 6: Perform and document a review to determine if the service provider's email services were used and move any emails that would be subject to FOIA requests or preserved in accordance with the EPA's Records Management Policy.

OW Response: The web service provider's email services were not used. All email regarding questions about PMOS or other communication were through the EPA contactor or EPA's mail system

Estimated Completion Date: 8/14/2015

CONTACT INFORMATION

If you have any questions regarding this response, please contact Thomas Dabolt, Director of OW's Project Management Office on (202) 564-1450 or Pravin Rana on (202) 564-1909.

Attachment

cc: Mike Shapiro
Albert Schmidt
Marilyn Ramos

Appendix D

Distribution

Office of the Administrator
Deputy Assistant Administrator for Water
Assistant Administrator for Administration and Resources Management
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 Public Affairs
Principal Deputy Assistant Administrator for Water
Principal Deputy Assistant Administrator for Administration and Resources Management
Principal Deputy Assistant Administrator for Environmental Information and Deputy Chief Information Officer
Director, Office of Wastewater Management, Office of Water
Director, Office of Acquisition Management, Office of Administration and Resources Management
Director, Office of Policy and Resource Management, Office of Administration and Resources Management
Deputy Director, Office of Policy and Resource Management, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of Water
Audit Follow-Up Coordinator, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of Environmental Information