UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

July 9, 2014

MEMORANDUM FOR KATHERINE ARCHULETA
Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Status of Cloud Computing Environments within OPM (Report No. 4A-CI-00-14-028)

The purpose of this memorandum is to communicate to you the results from our review of the contracts for cloud computing information systems used by the U.S. Office of Personnel Management (OPM). We submitted our conclusions and recommendations to OPM's Office of the Chief Information Officer (OCIO) representatives to elicit their comments. The OCIO's comments are included within this memorandum.

Executive Summary

Our review indicated that the language in OPM's current cloud computing contracts does not adhere to established best practices. We also determined that the Cloud Service Providers (CSP) hosting OPM systems are not certified or authorized in accordance with the Federal Risk and Authorization Management Program (FedRAMP) requirements.

As a result, we recommend that the contract language for cloud computing services be updated, and that OPM contract only with CSPs that are in compliance with FedRAMP.

Background

The OPM Office of the Inspector General (OIG) volunteered to participate in a government-wide review of cloud computing environments that was led by the Council of Inspectors General on Integrity and Efficiency. The review had two main purposes: 1) to review current agency cloud computing contracts for compliance with best practices established by the Chief Information Officers (CIO) Council and Chief Acquisition Officers Council and, 2) to determine if agency systems used FedRAMP to acquire and authorize cloud services.

Scope and Methodology

To perform our review we evaluated the contracts for a sample of OPM information systems that use CSPs to host applications. We also interviewed individuals from OPM's Contracting Office, program office officials that use cloud-based systems, and OPM's Chief Information Security Officer.

Our review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however, because we consider this to be a review, the documentation, reporting, and quality control standards are not as stringent.

Review Results

Our review indicated that OPM's cloud computing contracts do not adhere to established best practices. We also determined that CSPs hosting agency systems are not certified or authorized by FedRAMP.

a) Cloud Service Provider Procurement and Contract Formation

The CIO Council and Chief Acquisition Officers Council published a document titled "Creating Effective Cloud Computing Contracts for the Federal Government" that establishes best practices for acquiring information technology (IT) as a service. The document establishes the following areas that should be addressed when creating a cloud computing contract:

- Selecting a cloud service;
- CSP and end-user agreements;
- service level agreements;
- CSP, agency, and integrator roles and responsibilities;
- standards;
- security;
- privacy;
- e-discovery;
- Freedom of Information Act; and
- federal e-records management

We reviewed a sample of agency cloud computing contracts and determined that none of them incorporated all of these best practices. Over the last few years, the OCIO has worked with the Contracting Office to incorporate new language into contracts for IT services to enforce Federal Information Security Management Act requirements. However, the new language does not adequately address cloud services for the areas listed above.

Failure to incorporate cloud specific language into agency contracts has multiple risks. For instance, there is an increased risk that data ownership is not adequately established, which could allow a cloud provider to have unnecessary access to sensitive federal data. Also, failure to define security standards and testing requirements increases the risk of a data breach, which could lead to the loss or corruption of sensitive federal data.

Recommendation 1

We recommend that the OCIO work with OPM's Contracting Office to review cloud computing contract best practices, and incorporate appropriate language into future contracts for cloud services. We also recommend that the Contracting Office assess the feasibility of incorporating the updated contract language into existing contracts for cloud services.

OCIO Response:

"The CIO believes that while existing security contract language that goes into all IT contracts [is] aligned with OPM security policy and FISMA requirements, it would enhance security to incorporate additional language to specifically address Cloud environments."

OIG Reply:

As part of the recommendation resolution process, please provide OPM's Internal Oversight and Compliance division with evidence supporting the corrective action taken.

b) FedRAMP Compliance

In December 2011, the Office of Management and Budget (OMB) released a memorandum addressing the security authorization process for cloud computing services. The memorandum requires all federal agencies to use FedRAMP when procuring and subsequently authorizing cloud computing solutions effective June 5, 2014. Specifically, each agency must do the following:

- Use FedRAMP when authorizing cloud services;
- Use the FedRAMP process and security requirements as a baseline for authorizing cloud services;
- Require CSPs to comply with FedRAMP security requirements;
- Establish a continuous monitoring program for cloud services;
- Ensure that maintenance of FedRAMP security authorization requirements is addressed contractually;
- Require that CSPs route their traffic through a Trusted Internet Connection; and
- Provide an annual list of all systems that do not meet FedRAMP requirements to OMB.

We determined that no OPM cloud-based systems are currently using FedRAMP approved CSPs. However, several systems are using FedRAMP accredited third party assessment organizations to perform security control testing. While this type of testing does not satisfy FedRAMP requirements, it provides an additional level of assurance that the systems' security controls are adequately tested.

We reviewed OPM's Information Security and Privacy Policy Handbook to determine what guidance is available related to cloud computing. While cloud computing is addressed, FedRAMP requirements are not incorporated into OPM policy or procedures. We were told that the OCIO is in the process of updating the Information Security and Privacy Policy Handbook and that FedRAMP will be addressed, but they are not complete at this time. Failure to comply with FedRAMP requirements increases the risk that information systems' security controls will not be adequately tested, which could lead to a data breach and the loss or corruption of sensitive federal data.

Recommendation 2

We recommend that the OCIO update its cloud computing policies and procedures to incorporate FedRAMP requirements.

OCIO Response:

"Cloud Computing security policies are documented in the OPM Security Handbook. The available FedRAMP material on cloud computing [consists] of procedures and templates which typically would not be added to a security policy. We will review the FedRAMP Material and make a determination how best to incorporate [it] into OPM security procedures."

OIG Reply:

While we agree that cloud computing security policies are documented in the OPM Information Security and Privacy Policy Handbook, FedRAMP requirements are not addressed. At a minimum, we would expect the policy to require all agency systems to use FedRAMP compliant CSPs when acquiring cloud services.

Recommendation 3

We recommend that the OCIO require all program offices with cloud-based systems to use CSPs that are FedRAMP compliant.

OCIO Response:

"It's our policy to use FedRAMP Cloud Service Providers (CSP) for new or renewing cloud services when feasible. FedRAMP CSPs are currently accredited at the FIPS-199 moderate level and therefore cannot host OPM's high systems. There is also the issue [of] FedRAMP delays in [processing] applications for new cloud services and the impact on the ability for program offices to execute their missions. We have approached FedRAMP in the past to host OPM systems and [were] told that it would take almost a year to join the program because of a backlog of agencies waiting to join the program."

OIG Reply:

We understand that the process for a CSP to obtain FedRAMP compliance takes time and that it may be difficult for a program office to change CSPs. However, the OMB memorandum establishing FedRAMP and the requirement that each agency use FedRAMP compliant CSPs was published in December 2011. The intent of the recommendation is for OPM to enforce the requirements established by OMB.

Please contact me on 606-1200 if you have any questions, or your staff may wish to contact Michael R. Esser, Assistant Inspector General for Audits, on [redacted].

cc: Ann Marie Habershaw
Chief of Staff and Director of External Affairs

Donna K. Seymour
Chief Information Officer

Mark W. Lambert
Associate Director
Merit Systems Accountability and Compliance

Janet L. Barnes
Director
Internal Oversight and Compliance

[redacted]
Chief, Policy and Internal Control