Audit Report

OIG-15-003

INFORMATION TECHNOLOGY: Fiscal Service's Management of Cloud Computing Services Needs Improvement

October 8, 2014

Office of Inspector General

Department of the Treasury

Contents

Audit Report

Appendices

Abbreviations and Acronyms

AO	Authorizing Official
ATO	Authorization to Operate
COR	Contracting Officer's Representative
FedRAMP	Federal Risk and Authorization Management Program
Fiscal Service	Bureau of the Fiscal Service
FMCS	Federal Managed Cloud Services
GSA	General Services Administration
NIST	National Institute of Standards and Technology
OeBS	Oracle eBusiness Suite
OIG	Treasury Office of Inspector General
OMB	Office of Management and Budget
Treasury	Department of the Treasury

This Page Intentionally Left Blank

October 8, 2014

Sheryl Morrow
Commissioner, Bureau of the Fiscal Service

Raghav Vajjhala
Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer

This report represents the results of our audit of the security over public clouds used by the Department of the Treasury (Treasury). The overall objective of this audit was to determine whether Treasury ensured effective security protection of its information on public clouds maintained by contractors as required by federal policies, guidelines and contracts. This report focused on the Bureau of the Fiscal Service's (Fiscal Service) use of Oracle's Federal Managed Cloud Services (FMCS) which was selected for audit based on the financial management support Fiscal Service provides to Treasury bureaus and other Federal agencies.

To accomplish our audit objective, we surveyed Treasury bureaus and offices to assess how cloud computing had been utilized; interviewed key officials and personnel at Fiscal Service and Oracle; reviewed and analyzed security-related documentation; and performed physical security testing. We performed our fieldwork in Reston, Virginia, and Austin, Texas, between August 2013 and February 2014. Appendix 1 provides more detail on our objective, scope, and methodology.

Results in Brief

We determined that Oracle had security controls in place to protect its FMCS infrastructure although six Federal Risk and Authorization Management Program (FedRAMP)[1] controls were not in place at the time of our audit. Oracle already had a Plan of Action and Milestones (POA&M)[2] item for five of these controls and accepted the risks for the remaining control. Furthermore, Oracle received a provisional Authorization to Operate (ATO)[3] for FMCS from FedRAMP's Joint Authorization Board[4] in February 2014. The lack of these FedRAMP controls did not prevent Oracle from receiving a provisional ATO; therefore, we do not have any findings related to them.

With regard to Fiscal Service, we found that management did not grant an agency ATO for use of Oracle's FMCS as required by FedRAMP. Furthermore, Fiscal Service's task order with Mythics, a reseller of Oracle's cloud services, did not include terms for requiring compliance with FedRAMP security authorization requirements as directed by the Office of Management and Budget (OMB). As another matter concerning the task order with Mythics, we found that it contained certain terms for conducting audits involving Oracle that limited our access to Oracle's facilities and records. While this did not, in the end, limit the scope of our audit, it did cause significant delays in completing our work.

---

[1] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
[2] A POA&M is a list of deficiencies in a system and tracks their resolution.
[3] OMB Memorandum (December 8, 2011), Security Authorization of Information Systems in Cloud Computing Environments, "Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan".
[4] The FedRAMP Joint Authorization Board is the primary governance and decision-making body for the FedRAMP program, and they review and provide joint provisional security authorizations of cloud solutions, using a standardized baseline approach.

Overall, we are making five recommendations to management to ensure FedRAMP compliance by both Fiscal Service and Oracle. We recommend that Fiscal Service ensure a review of Oracle's FedRAMP security authorization package is performed to determine if risks are acceptable for granting an agency ATO and update its policies and procedures to include all FedRAMP requirements for granting an agency ATO. With regard to Fiscal Service's contracting for cloud services, we recommend that all current and future contracts and task orders for cloud services include terms specifying FedRAMP compliance. We also recommend that Fiscal Service remind staff and contractors of OIG's oversight authority and that OIG is not subject to terms and conditions in any Fiscal Service contract or task order. Finally, we recommend that policies and procedures be updated to include a requirement that contracts and task orders for cloud services include terms specifying compliance with FedRAMP security requirements.

In a written response, management generally agreed with our recommendations to ensure FedRAMP compliance for use of its current cloud services and when contracting for such services going forward. Management's response overall provided detailed corrective actions to our recommendations; however, we noted that some of the proposed actions did not fully address all recommendations. With regard to ensuring future FedRAMP compliance, the response did not provide a detailed plan for granting an agency ATO specific to Fiscal Service's current cloud services with Oracle. In addition, management did not commit to updating its policies and procedures to include terms specifying compliance with FedRAMP security requirements in contracts and task orders for cloud services.

Lastly, we appreciate management's recognition of the OIG's statutory authority and its willingness to work with our office to ensure access to both Fiscal Service and its contractors. We have summarized and evaluated management's response in the recommendation sections of this report. Management's response is provided in appendix 2.

Background

Cloud computing is the use of computing resources that are delivered as a service over a network. It is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources which includes networks, servers, storage, applications, and services. These resources can be rapidly created, rearranged, or removed with minimal management effort or service provider interaction. Cloud services are attractive because they can result in lower total cost of ownership and increase operational performance in the areas of availability, security, and scalability.

Treasury uses cloud services for various applications within Departmental Offices and component entities. In the case of Fiscal Service, cloud-based hosting and maintenance is used to provide financial management services to Treasury components and other Federal entities. Fiscal Service's mission is to "promote the financial integrity and operational efficiency of the Federal government through exceptional accounting, financing, collections, payments, and shared services." Fiscal Service uses Oracle's E-Business Suite of applications running on FMCS, a "community cloud," where some of the resources are shared with other Federal agencies. Oracle's cloud infrastructure physically resides at Oracle's Austin, Texas, data center.

In 2008, Fiscal Service signed a task order under General Services Administration's (GSA) contract with Immix, a reseller of Oracle's hosting and infrastructure support services. Since GSA's contract expired in 2013, Fiscal Service signed a new task order under GSA's contract with Mythics, another reseller of Oracle's cloud services. Specifically, these resellers provide access to Oracle's hosting services such as applications management, operations and maintenance, infrastructure support, disaster recovery, and security for various complex systems.

In December 2011, OMB issued a memorandum to Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing Environments," (hereinafter

referred to as OMB's FedRAMP memorandum), creating FedRAMP as a program that would provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services within the Federal Government. This approach uses a "do once, use many times" framework that saves cost, time, and staff that would be required to conduct redundant agency security assessments. FedRAMP became operational on June 5, 2012, at which point compliance became mandatory for all new cloud services. Pre-existing services, or those in the process of procurement, had until June 5, 2014, to become fully compliant. In addition, agencies were required to grant an agency ATO for use of cloud services.

Results of Audit

Finding 1 Agency ATO Was Not Issued for Use of Oracle's Cloud Services

Fiscal Service did not issue an agency ATO for the use of Oracle's FMCS by OMB's June 5, 2014, deadline for agencies' existing cloud services to become FedRAMP compliant. Furthermore, Fiscal Service did not include a requirement for an agency issued ATO in its policies and procedures. While Fiscal Service had reviewed and accepted the risks from previous versions of Oracle's FMCS Security Assessment and Authorization (SA&A)[5] package, this SA&A package pre-dated the stricter FedRAMP security controls. FedRAMP requires stricter controls in areas such as access control, security assessments, vulnerability scanning, and cryptographic keys.

According to the Fiscal Service Contracting Officer's Representative (COR), a determination was made at the time the original task order with Immix was put in place that Fiscal

[5] An SA&A package consist of control testing and documentation that is reviewed in the process of issuing an ATO determination.

Service, as a Federal entity, could not provide an ATO for a corporation and its activities authorizing it to operate on Fiscal Service's behalf. However, FedRAMP requires that the agency issue an agency ATO for its use of a cloud service which is different than an ATO to the provider to operate a cloud service. To issue an agency ATO, an agency can either leverage an existing security authorization package that FedRAMP used for granting its provisional ATO or create its own package following the FedRAMP assessment process. It is the agency's Authorizing Official (AO) who makes the final decision to grant an agency ATO after reviewing the security assessment package and determining that it is complete, consistent, and compliant with FedRAMP requirements.

As a result of not completing the review of the more stringent security controls included in the FedRAMP security authorization package, the AO may not be aware of new risks introduced by Oracle's changes to FMCS' systems controls for becoming FedRAMP compliant.

Recommendations

We recommend that the Commissioner of Fiscal Service:

1. Ensure a review of the FedRAMP security authorization package is performed on Oracle's FMCS for determining whether the risks of using Oracle's cloud services are acceptable for granting an agency ATO.

   Management Response

   Management agreed with our assessment that an agency ATO for the use of Oracle's FMCS had not been issued by OMB's June 5, 2014 deadline for agencies' existing cloud services to become FedRAMP compliant. Management explained that its OeBS [Oracle eBusiness Suite] is hosted on Oracle's FMCS cloud environment which Fiscal Service assesses and authorizes as part of the OeBS boundary. Fiscal Service migrated hosting of OeBS to Oracle on Demand (currently FMCS) with an initial ATO on April 3, 2009 which covered the OeBS

boundary and took into consideration risks associated with controls inherited from FMCS. Management also stated that it reviewed Oracle's FMCS FedRAMP provisional ATO and subsequently requested access to the package in the FedRAMP repository. Management plans to leverage the provisional ATO and any continuous monitoring results as part of the upcoming annual SA&A scheduled for completion by April 3, 2015.

OIG Comment

Management agreed with our recommendation, and its planned corrective action includes a review of the FedRAMP security authorization package as recommended. However, its response did not address granting FMCS an ATO separate from OeBS. Therefore, we reiterate the second part of our recommendation that management determine whether the risks are acceptable for granting an agency ATO specifically for the use of FMCS.

2. Ensure that policy and procedures are updated to include all FedRAMP requirements for granting an agency ATO for the use of all cloud services.

Management Response

Management stated that it will review its policies and procedures regarding cloud environments to ensure FedRAMP requirements for authorization are clearly articulated.

OIG Comment

Management's response meets the intent of our recommendation.

Finding 2 Fiscal Service Did Not Ensure FedRAMP Compliance When Contracting for Cloud Services

Under GSA's contract with Oracle reseller Mythics, Fiscal Service signed a task order in February 2013 for the use of Oracle's FMCS. However, neither GSA's contract nor Fiscal Service's task order contained clauses requiring Oracle's cloud services to be FedRAMP compliant. We also noted that Fiscal Service did not update its policies and procedures to ensure FedRAMP compliance of cloud services that might be obtained through third-party providers.

In its FedRAMP memorandum, OMB directed agencies to ensure that applicable contracts require cloud service providers to comply with FedRAMP security authorization requirements. According to the Fiscal Service COR, there were no hosting agencies that were FedRAMP certified when soliciting for cloud services in November 2012. Although Oracle was in the process of seeking FedRAMP certification, no one knew a time frame by which it would be accomplished. Nevertheless, FedRAMP was a known future requirement as of OMB's December 2011 FedRAMP memorandum. Therefore, we believe that Fiscal Service had the opportunity to include FedRAMP security requirements and compliance in its task order with Oracle's reseller Mythics given that the task order included option years falling within the FedRAMP compliance periods.

Without specifically requiring FedRAMP compliance in the task order with Mythics, Fiscal Service is unable to enforce FedRAMP compliance for Oracle's FMCS. Prior to FedRAMP granting Oracle a provisional ATO in February 2014, FMCS was implemented with baseline security requirements prescribed by NIST[6] and did not include the more stringent FedRAMP controls for cloud systems.

[6] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations (August 2009)

Recommendations

We recommend that the Commissioner of Fiscal Service:

1. Ensure all current and future contracts and task orders for cloud services, including the current task order with Mythics, require FedRAMP compliance.

   Management Response

   Management stated that it will immediately begin the process of modifying the current task order with Mythics to include FedRAMP compliance. Management also plans to take the necessary steps to identify and review applicable contracts and task orders that were put in place prior to FedRAMP to ensure that compliance is in place or still required. As such, bilateral modifications will be put in place for those contracts and task orders that do not currently include mandatory FedRAMP compliance requirements. Management noted that the process of identifying, reviewing, and modifying applicable contracts will begin immediately.

   OIG Comment

   Management's response meets the intent of our recommendation.

2. Ensure policies and procedures are updated to include a requirement that contracts and task orders for cloud services include terms specifying compliance with FedRAMP security requirements.

   Management Response

   Management responded that it will enhance the annual COR Refresher training to include a more in-depth discussion about FedRAMP compliance and contract requirements. Management also plans to include language about FedRAMP compliance and responsibilities in the next revision of the COR Designation Letter. Management indicated that the standard FedRAMP compliance

language is included in new Fiscal Service solicitations and awards.

OIG Comment

We acknowledge and support management's planned efforts to strengthen COR training on FedRAMP and contract requirements. However, the response did not specify action with regard to updating policies and procedures to include FedRAMP compliance when contracting for cloud services. Therefore, we reaffirm our recommendation to ensure FedRAMP compliance be documented as a matter of policy.

Finding 3 Fiscal Service's Task Order with Mythics Restricted Audit Access

Fiscal Service's task order with Mythics contained terms for providing audit support that caused significant delays in receiving critical documents and gaining access necessary to perform physical security testing at Oracle facilities. Fiscal Service attempted to apply those restrictions to our audit which were in violation of our authority as an independent Treasury unit to conduct audits under the Inspector General Act of 1978, as amended.[7] Furthermore, as an independent unit, we were not party to the task order, and therefore, not subject to its terms.

Fiscal Service initially required that we adhere to the task order's 6-week turn-around for any data calls regarding access to Oracle. Furthermore, the task order allowed for only two non-regulatory audits per year with no additional charge to Fiscal Service. Since Fiscal Service had already scheduled access to Oracle for the first week of November and May, we were expected to follow these timeframes so as to not incur additional costs to Fiscal Service. As a result, it took approximately 2 months to gain access to Oracle documents

[7] Pub. L. 95-452 (Oct. 12, 1978)

after our initial data call in August 2013. Given that we had only one week available in November 2013 to perform our on-site review of Oracle's documents, we re-prioritized other ongoing audits to reallocate resources to ensure all critical documents were reviewed and analyzed.

When we inquired as to why the task order with Mythics contained certain audit conditions, the Fiscal Service COR told us that the contract and the service descriptions clearly state that Oracle acknowledges the right of third parties to review and audit as required by law. The COR also noted that there were no issues in the past adhering to the contract and service descriptions under which a review or audit is to be requested and scheduled with Oracle resources. Although we were mindful of staff resources and time at both Fiscal Service and Oracle during our audit, we would like to continue to remind management that audits conducted by the OIG cannot be restricted by terms in a contract or task order.

Recommendation

We recommend that the Commissioner of Fiscal Service:

1. Remind staff and contractors of the OIG's oversight authority under the Inspector General Act of 1978, as amended. As such, the OIG is not subject to terms and conditions in any Fiscal Service contract or task order.

   Management Response

   Management recognized the OIG's statutory authority to conduct audits and that OIG is not subject to terms and conditions of contracts or task orders which Fiscal Service may enter into. Management pointed out that nothing in the Mythics contract restricted OIG's access to contractor information. In addition, Attachment A of the Mythics contract included a clause providing that the contractor shall be subject to periodic audits and reviews, as required by law, such as OIG audits. Management affirmed that Fiscal Service will work with OIG to ensure

access to Fiscal Service and contractor facilities and documents.

OIG Comment

We appreciate management's acknowledgement of OIG's statutory authority and its willingness to work with our office to ensure access to both Fiscal Service and its contractors. We also recognize that Mythic's task order did not specifically restrict our office's access to the contractor's information. Nevertheless, we would like to point out that the task order did contain other general audit restrictions as discussed in our finding that Fiscal Service staff and Oracle contractors attempted to apply to this audit. Therefore, we reiterate our recommendation that management remind staff and contractors of the OIG's oversight authority and its exemption from being held to the terms and conditions of any Fiscal Service contract or task order.

* * * * * *

I would like to extend my appreciation to the Fiscal Service staff for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-5171 or Larissa Klimpel, Audit Manager, Information Technology Audit, at (202) 927-0361. Major contributors to this report are listed in appendix 3.

/s/

Tram Jacquelyn Dang
Director, Information Technology Audit

In October 2012, we initiated an audit of the security controls over the Department of the Treasury's (Treasury) information on public clouds. The overall objective of this audit was to determine whether Treasury ensured effective security protection for its information on public clouds maintained by contractors as required by federal policies, guidelines and contracts.

As part of our audit, we surveyed Treasury's bureaus and offices to determine how cloud computing had been utilized. We considered such factors as number and type of users, type of cloud service, and significance of data processed. Based on the results of our survey, we selected the Bureau of the Fiscal Service's use of Oracle's Federal Managed Cloud Services (FMCS) for review because of the financial management support it provides to Treasury bureaus and other Federal agencies.

To accomplish our audit objectives, we interviewed key officials and personnel at Fiscal Service; reviewed key documents including Fiscal Service's task order with Mythics, the reseller of Oracle's cloud services; visited Oracle's facilities in Reston, Virginia, and Austin, Texas, where we interviewed staff, reviewed and analyzed security-related documents; and inspected the physical security around systems storing Treasury data. We performed our fieldwork between August 2013 and February 2014.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

COMMISSIONER

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
WASHINGTON, DC 20227

September 26, 2014

Ms. Tram Dang
Director, IT Audits
U.S. Department of the Treasury
Office of the Inspector General
JBAB Building 410/Door 123
250 Murray Lane, SW
Washington, DC 20222

Ms. Tram Dang:

Thank you for the opportunity to respond to the Treasury Office of Inspector General (OIG) formal draft audit report, *Information Technology: Fiscal Service's Management of Cloud Computing Services Needs Improvement*, dated September 16, 2014. Our responses to the five recommendations are as follows and activities for which action will be taken will be documented in a planned corrective action plan:

1. Ensure a review of the FedRAMP security authorization package is performed on Oracle's Federal Managed Cloud Services (FMCS) for determining whether the risk of using Oracle's cloud services is acceptable for granting an agency ATO.

   Fiscal Service agrees with the OIG's assessment that an agency Authority to Operate (ATO) for the use of Oracle's FMCS had not been issued by OMB's June 5, 2014, deadline for agencies' existing cloud services to become FedRAMP compliant. Fiscal Service is committed to ensuring the security of its information systems. Fiscal Service has robust processes in place to ensure that security controls for its systems, including those provided by third-parties, address Treasury and Fiscal Service's stringent security control baselines. Furthermore, Fiscal Service maintains that the security controls in place for the Oracle e-Business Suite (OeBS) system have been and continue to be appropriate and adequate.

   Fiscal Service's OeBS system is hosted on Oracle's FMCS cloud environment which received a FedRAMP JAB Provisional ATO (P-ATO) on February 24, 2014. Fiscal Service assesses and authorizes the Oracle environment as part of the OeBS authorization boundary. Fiscal Service migrated hosting of OeBS to Oracle on Demand (currently FCMS) with an initial ATO on April 3, 2009. The ATO covered the OeBS boundary, which included Fiscal Service's dedicated infrastructure and application controls, taking into consideration risks associated with controls inherited from Oracle's shared infrastructure (FMCS). At that time,

and annually thereafter, Oracle contracted with a third party assessor to have an independent National Institute of Standards and Technology (NIST) compliant 800-53A assessment completed on the shared infrastructure, which Fiscal Service leveraged as part of OeBS' security assessment and authorization (SA&A) and continuous monitoring activities. This approach is in accordance with guidance issued by the Fiscal Service Chief Information Security Officer in September 2013, "Strategy for obtaining assurance that IT security controls employed by service providers are operating effectively." The OeBS system has been authorized annually by a Fiscal Service Authorizing Official since 2009.

In June 2014, Fiscal Service reviewed Oracle's FMCS FedRAMP P-ATO and has subsequently requested access to the package in the FedRAMP repository. The P-ATO and any continuous monitoring results will be leveraged as part of the upcoming annual SA&A scheduled for completion by April 3, 2015.

2. Ensure that policy and procedures are updated to include all FedRAMP requirements for granting an agency ATO for the use of all cloud services.

   Fiscal Service will review its policies and procedures in regards to cloud environments to ensure FedRAMP requirements for authorization are clearly articulated.

3. Ensure all current and future contracts and task orders for cloud services, including the current task order with Mythics, requires FedRAMP compliance.

   Fiscal Service is committed to ensuring the security of its information systems. Fiscal Service includes compliance with Federal, Treasury, and Fiscal Service security requirements in its solicitations and awards. Fiscal Service will immediately begin the process of modifying the current task order with Mythics to include this requirement. Fiscal Service will take the necessary steps to identify applicable Fiscal Service contracts and task orders that were put in place prior to the FedRAMP compliance requirement. These contracts and orders will be reviewed to ensure that FedRAMP compliance is currently in place or is still required. Bilateral modifications will be put in place for Fiscal Service applicable contracts and task orders that do not currently include mandatory FedRAMP compliance requirements. The modifications will be signed by the Contracting Officer and the contractor and require that the contractor comply with the FedRAMP security authorization requirements. The process of identifying applicable contracts, reviewing for compliance, and modifying (where applicable) will begin immediately.

4. Ensure policies and procedures are updated to include a requirement that contracts and task orders for cloud services include terms specifying compliance with FedRAMP security requirements.

Fiscal Service will enhance the yearly COR Refresher training to include a more in depth discussion about FedRAMP compliance and contract requirements. Language about FedRAMP compliance and responsibilities will also be included in the next revision of the COR Designation Letter. The standard FedRAMP compliance language is included in new Fiscal Service solicitations and awards.

5. Remind staff and contractors of the OIG's oversight authority under the Inspector General Act of 1978, as amended. As such, the OIG is not subject to terms and conditions in any Fiscal Service contract or task order.

   Fiscal Service recognizes that OIG has the statutory authority to conduct audits under the Inspector General Act of 1978, as amended, and that OIG is not subject to terms and conditions of contracts or task orders which Fiscal Service may enter into. To that end, we would note that nothing in the Mythics contract restricts OIG's access to contractor information. In addition, Attachment A of the Mythics contract contains a clause providing that the contractor shall be subject to periodic audits and reviews, as required by law, such as OIG audits. Fiscal Service will work with OIG to ensure that OIG has access to Fiscal Service and contractor facilities and documents.

If you have any questions or wish to discuss these comments in more detail, please contact Deputy Commissioner Kimberly McCoy or me on (202) 874-7000.

Sincerely,

Sheryl R. Morrow

Office of Information Technology (IT) Audit

Tram J. Dang, Director
Larissa Klimpel, Audit Manager
Robert Kohn, Auditor-in-Charge
Jason Beckwith, IT Specialist
Dan Jensen, IT Specialist
Don'te Kelley, IT Specialist
Mitul "Mike" Patel, IT Specialist
James Shepard, Referencer

The Department of the Treasury

Acting Deputy Assistant Secretary Information Systems and Chief Information Officer

Office of Strategic Planning and Performance Management

Risk and Control Group, Office of Deputy Chief Financial Officer

Bureau of the Fiscal Service

Commissioner

Chief Internal Control Officer

Office of Management and Budget

OIG Budget Examiner