INSPECTION

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Cloud Computing Security Documentation in the Cyber Security Assessment Management Solution

Report No.: 2015-ITA-017

November 2015

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

NOV 12 2015

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall Mary L Kendall
Deputy Inspector General

Subject: Inspection Report – Cloud Computing Security Documentation in the Cyber Security Assessment Management Solution
Assignment No. 2015-ITA-017

We inspected the completeness and adequacy of required information technology (IT) security documentation for a sample of U.S. Department of the Interior (Department) IT systems that had been moved to a public cloud. The inspection focused on: 1) whether the sampled cloud computing systems were recorded in the Cyber Security Assessment Management Solution (CSAM), and 2) if CSAM entries met Department and Federal security documentation requirements.

We sampled 16 of 26 operational systems reported by the Department: 1 from the Bureau of Ocean Energy Management, 2 from the Bureau of Safety and Environmental Enforcement, 3 from the U.S. Bureau of Reclamation, and 10 from the U.S. Geological Survey.

We issued three Notices of Potential Finding and Recommendations (NPFRs) and received bureau responses to our NPFRs' recommendations. Based on our findings, we are making seven recommendations to strengthen the Department's IT security program, and close identified security gaps.

Please provide us with your written response to this report within 30 days. The response should provide detailed information on actions you have taken or plan to take to address each recommendation, as well as target dates and titles of the officials responsible for implementing these actions. Please address your response to:

Kimberly Elmore
Assistant Inspector General
Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428
1849 C Street, NW.
Washington, DC 20240

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief

We conducted this inspection to determine the completeness and adequacy of required information technology (IT) security documentation for 16 IT systems that the Bureaus of Reclamation (USBR), Safety and Environmental Enforcement (BSEE), and U.S. Geological Survey (USGS) had moved to a public Cloud. USBR and USGS did not meet the U.S. Department of the Interior's (Department's) policy for maintaining required IT security documentation. Specifically, USBR had not completed any security documentation for its three operational Cloud systems. As such, these systems were operating without authorization, placing bureau data in the Cloud potentially at risk of unauthorized access, disclosure, modification, or destruction.

While we found that USGS had moved its data to the Cloud in early 2013, it had not completed necessary security documentation until late 2014. These deficiences possibly occurred because the Office of Chief Information Officer (OCIO) did not effectively oversee the bureaus to ensure that operational Cloud systems met required IT security reqirements.

We make seven recommendations to OCIO and affected bureaus to strengthen oversight of the Department's IT security program and close identified security gaps.

Introduction

Objective

To determine if the U.S. Department of the Interior's (Department's) security documentation for Cloud computing systems was complete by determining: 1) whether the bureaus recorded their operational Cloud systems in the Cyber Security Assessment Management system[1] (CSAM), and 2) if CSAM entries met Department and Federal security documentation requirements.

Background

A public Cloud is a shared, Internet-accessible computing environment operated by a Cloud service provider such as Amazon or Microsoft. Cloud based IT systems have the same Federal and Department security requirements as systems managed by bureau personnel and operated by a departmental data center.

As of September 2014, the Department reported it had contracted for 26 operational Cloud computer information systems. In addition, it projects significant increases in future Cloud usage, with up to 100 percent of new IT programs potentially beginning in the Cloud, and nearly all of the Department's current or legacy systems, as well as public data, likely to be moved to the Cloud.

The Department's Office of the Chief Information Officer (OCIO) requires bureaus to use CSAM as its database for information systems, including Cloud computing information systems. OCIO requires that specific security documentation for each information system be placed in CSAM.[2] The documentation required includes a system's security plan, security configurations, continuous monitoring strategy, contingency plans, configuration management plan, risk assessments, plan of action with milestones, and authorization decision documents.

CSAM must contain all of the Department's computer systems in order to support the annual evaluations required by the Federal Information System Management Act (FISMA).[3] Systems need to have the required security information so that system owners and authorizing officials have the relevant information to support continuous monitoring, and meet the requirements of FISMA's annual assurance statements.

To help Federal agencies meet "Cloud First" requirements, the General Services Administration, in collaboration with several other agencies, established the Federal Risk Authorization Management Program (FedRAMP). FedRAMP helps

[1] The Cyber Security Assessment Management solution is a software database system used to store the Department's computer security documentation.

[2] Department of Interior, Office of Chief Information Officer Directive 2011-006, "Information System Boundary Assessment & Authorization Package Documentation and Inventory," March 23, 2011.

[3] The Federal Information Security Management Act (FISMA) of 2002 requires an annual, independent evaluation of agencies' information security programs and practices.

agencies adopt Cloud computing technologies by (1) ensuring that Cloud providers have adequate IT security, (2) eliminating duplication of effort and reducing risk management costs, and (3) enabling rapid and cost-effective purchasing of Cloud computing services. As of June 2014, agencies are required to use only FedRAMP-approved Cloud service providers.

The Department has also mandated its Cloud First policy.[4] The Department is transitioning from owning and operating its entire IT infrastructure to using Cloud services. The January 2014 Cloud First policy memorandum notes the Department's "Cloud Strategy" is key to transforming the Department's IT capabilities into a modern Cloud based environment. Central to this strategy is the use of a Department contracting vehicle for future IT hosting procurements. The goal is to reduce the total cost of ownership of enterprise hosting hardware, software, and IT operations; and to provide greater service, security, and end-user support.

OCIO oversees bureau compliance for using CSAM. The Internal Control, Audit, and Compliance Management Division (ICACMD) in OICO is responsible for ensuring that bureaus meet Department and Federal information technology security requirements.

[4] Memorandum from Chief Information Officer and Director of the Office of Acquisition and Property Management and Senior Procurement Executive, Subject: Mandatory Use Policy for the Department of the Interior Foundation Cloud Hosting Services Contracts, dated January 6, 2014.

Findings

Of the 16 cloud computing systems we reviewed during our inspection, we found no security documentation for the 3 USBR systems, complete but not timely documentation for the 10 USGS systems, and complete and timely documentation for the 3 BOEM/BSEE systems. Not having complete and timely documentation for these cloud systems not only doesn't meet the requirements of FISMA’s annual assurance statements, but places Bureau data at risk of unauthorized access, disclosure, modification, or destruction. We believe the Department's OCIO plays a key role in ensuring cloud systems compliance, and as such, needs to strengthen its oversight in this area.

USBR’s Documentation in CSAM is Incomplete

The Bureau of Reclamation (USBR) operated three Cloud computing systems without any security documentation or records placed in CSAM. USBR security managers stated that they were unaware of these systems; consequently, they had not done proper security planning, completed required security documents, or formally authorized the systems for operation. Accordingly, USBR’s Cloud computing systems could be subject to unauthorized access, modification, or undetected destruction.

USBR shared one of its Cloud systems with eight other entities, including Federal, State, county, and tribal units. USBR personnel stated they were not aware of which entity had security responsibilities, or if security responsibilities were shared. FedRAMP specifies how to implement a shared Cloud computing system among several agencies. Specifically, one of the agencies acts as a sponsor and is then responsible for obtaining an authorization to operate. The other participating agencies may choose to leverage the sponsoring agency’s authorization to operate, or conduct their own security assessment work.

USBR’s noncompliance with FedRAMP occurred because the responsible USBR officials said they had not conducted security planning and documentation, and, therefore, had not placed security documentation in CSAM as required. We issued a “Notice of Potential Findings and Recommendations” (NPFR) to USBR with three recommendations. USBR concurred with the recommendations that were in the NPFR and that follow.

Recommendations

We recommend that USBR's Chief Information Security Officer:

1. Prepare the appropriate security documentation for existing and planned Cloud computing systems, grant authority to operate as appropriate, and ensure required documents are added to CSAM.

2. Review FedRAMP for guidance, roles, and responsibilities when multiple Federal agencies implement a shared Cloud computing service.

3. Ensure all planned and operational Cloud computing services are reported to OCIO's ICACMD.

USGS's Documentation in CSAM was Incomplete

USGS combined its 10 Cloud systems into one CSAM boundary[5] because of their design and use. The Cloud computing systems were operational in 2013, but USGS did not timely update CSAM with a full set of security documents until December 2014. CSAM now contains the appropriate documentation.

We made one recommendation to USGS in an NPFR concerned with services reported to OCIO's ICACMD (see Recommendation 4 below). USGS concurred with this recommendation and noted that it has developed new internal processes for ensuring Cloud computing systems meet security requirements, and that it now has sufficient documentation within CSAM.

Recommendation

We recommend that USGS:

4. Ensure all planned and operational Cloud computing services are timely reported to OCIO's ICACMD.

Cloud Computing Governance Needs Strengthening

Overall, OCIO does not have adequate oversight of the Department's security documentation for Cloud systems. It is important for all departmental systems to have the required security information so that system owners and system authorizing officials can support continuous monitoring and annual assurance statements. If CSAM is incomplete, then the annual FISMA evaluation may misrepresent the status of the Department's security program. The deficiencies we identified occurred because neither the responsible bureaus nor the Department's

[5] Computer security boundaries are a set of systems under a single administrative control.

officials ensured that their Cloud computing systems met Federal and Department security protocols. In particular, Department security personnel need to better understand FedRAMP's stated roles and responsibilities when collaborating with other agencies.

We issued an NPFR to OCIO that contained four recommendations to help ensure bureau compliance with Federal and Department IT security requirements, and to strengthen OCIO oversight of bureau practices related to Cloud computing. OCIO concurred with two recommendations directing bureaus to update CSAM and review FedRAMP roles and responsibilities to ensure Cloud systems meet applicable IT security requirements.

Based on OCIO's response to our other two preliminary recommendations, we withdrew one, which required bureaus to biannually report to OCIO all planned and operational Cloud computing systems as OCIO already requires such reporting. Finally, we reworded our last recommendation to strengthen the Department's IT governance by having OCIO reevaluate and enhance its IT security oversight practices.

Recommendations

We recommend that OCIO: direct responsible Bureau information technology staff to:

5. Update CSAM for all planned and operational Cloud computing systems.

6. Review specific FedRAMP roles and responsibilities for authorizing Cloud computing systems.

We recommend that OCIO:

7. Direct ICACMD to reevaluate and enhance its oversight, monitoring, and testing processes, to include periodic reviews to ensure bureaus comply with OCIO Directive 2011-006.

Conclusion

The bureaus need to evaluate systems to ensure they are following Federal guidelines, including FedRAMP. They have the responsibility to upload current and accurate security documentation into CSAM. OCIO needs to monitor CSAM regularly to ensure the bureaus timely upload the required security documentation. Although ICACMD oversees this area, it must improve its oversight to ensure a complete inventory is maintained. For example, our findings show that the current practice of bureau self-reporting Cloud systems is ineffective and increases the risk of unauthorized access to Department Cloud systems. In addition, the Department must keep an accurate inventory to have the required security information so that system owners and system authorizing officials have the relevant information to support continuous monitoring and, most importantly, meet the requirements of FISMA’s annual assurance statements.

As a result of OMB’s Cloud First policy, the Department has also implemented a mandatory policy to move IT into a modern Cloud based environment. The Department’s goal is to reduce the total cost of owning enterprise hosting hardware, software, and IT operations, while providing greater service, security, and end-user support.

Our findings relating to deficiencies in operating Cloud systems show the need for the Department to strengthen its governance over Cloud systems to ensure that the Department meets its IT security requirements for this new paradigm. The bureaus need to improve uploading security documentation into CSAM and OCIO needs to improve its oversight of the bureaus’ use of CSAM.

Appendix 1: Scope and Methodology

Scope

We limited our inspection to a judgmental sample of 16 of the 26 operational Cloud information systems reported by the U.S. Department of the Interior.

Methodology

The Department's policy for using the Cyber Security Assessment Management system (CSAM) specifies that each computer system's security documentation must be posted in CSAM.[6] Required documentation includes the system's security plan, security configurations, continuous monitoring strategy, contingency plans, configuration management plan, risk assessments, plan of action with milestones, and authorization decision documents. We identified each of the sampled Cloud systems in CSAM, and looked at their documentation to assure that the documents met Federal and departmental requirements.

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

We interviewed bureau and Department staff to determine the processes and guidance they were following. We reviewed the DOI Cloud First policy and Federal policy documentation to determine best practices.

[6] Department of Interior Office of Chief Information Officer Directive 2011-006, "Information System Boundary Assessment & Authorization Package Documentation and Inventory," March 23, 2011.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doi.gov/oig/index.cfm

By Phone:

24-Hour Toll Free:	800-424-5081
Washington Metro Area:	202-208-5300

By Fax: 703-487-5402

By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240