Office of Audits
Office of Inspector General
U.S. General Services Administration

IMPLEMENTATION REVIEW OF ACTION PLAN

Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment

Report Number A140157/O/R/F15002
January 29, 2015

Assignment Number A160045
January 26, 2017

Table of Contents

Introduction 1

Results

Finding 1 – GSA could not provide signed MOUs to support that Google Sites owners accepted responsibility for operating and managing their sites 3

Finding 2 – GSA could not provide evidence to prove that it had performed the actions it outlined to notify individuals identified as being at high or moderate risk for identity theft..... 4

Conclusion..... 6

Appendixes

Appendix A – Report Distribution..... A-1

Introduction

We have completed an implementation review of the management actions taken in response to the recommendations contained in our January 2015 audit report, *Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment*. The contents of this report do not reflect a new security event. The original report was previously restricted for security reasons. These restrictions no longer apply because the related security issues have been resolved.

Objective

The objective of our review was to determine whether the Office of GSA IT (GSA IT) has taken the corrective actions as outlined in the action plan for *Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment*. To accomplish our objective we:

- Examined documentation submitted by GSA IT supporting completion of the action plan steps;
- Performed limited testing of the corrective actions outlined in the action plan; and
- Interviewed and corresponded with GSA IT personnel.

Background

On January 29, 2015, we issued an audit report, *Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment*, to GSA IT. The objectives of our audit were to evaluate the nature and types of personally identifiable information (PII) contained in GSA's Google cloud computing environment, establish whether GSA properly protected PII, and determine if the measures taken by GSA to notify individuals affected by the exposure of their PII were adequate. We identified access control weaknesses in GSA's Google cloud computing environment, which contained approximately 3.8 million documents. GSA IT determined that at least 907 government employees, contractors, and job applicants had their PII compromised and were left vulnerable to the possibility of identity theft, harassment, embarrassment, or potential prejudice.

Our audit found:

- PII was accessible to employees and contractors without a valid need to know the information.
- Breach notifications to affected individuals were inadequate.

To address the issues identified in the report, we recommended that the Chief Information Officer/Senior Agency Official for Privacy and Chief Privacy Officer:

1. Restrict all content contained in GSA's cloud computing environment to the content's owner until:
    a. The sensitivity of the content has been evaluated and the sensitivity level documented;
    b. The relevance of any sensitive content has been evaluated based on current business needs, and content that is no longer needed has been removed;
    c. There has been confirmation that individuals with access to sensitive data have a valid need to know the information; and
    d. The content and access permissions have been certified and approved.
2. Reassess the privacy posture of GSA's cloud computing environment to determine if the level of risk is acceptable to authorize the system to operate.
3. Prohibit the posting of any new content to cloud applications until sufficient controls are established and implemented to ensure PII is properly protected and only accessible to individuals with a valid need to know such information. This includes considering adjusting default settings for cloud applications.
4. Reevaluate and recertify, on a routine basis, the sensitivity, relevance, and accessibility of all content contained in GSA's cloud computing environment.
5. Train GSA employees and contractors on the requirements for safeguarding PII that should include, but not be limited to, security requirements and responsibilities for PII in GSA's cloud computing environment and the proper setting of access controls to meet data security needs.
6. Monitor and manage access privileges to GSA's cloud computing environment on a continuous basis to ensure that documents containing PII are only available to users with a present and valid need to know such information.
7. Identify and inform affected individuals who have not yet been contacted regarding the breach, and amend the previous notifications. Ensure the notifications contain sufficient details about the breach, as specified in Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
8. Review and update GSA Order HCO 9297.2, *GSA Information Breach Notification Policy*, as necessary. Ensure the policy incorporates a structured response time schedule for notifying affected individuals for all suspected and confirmed breaches.

GSA management agreed with our recommendations.

Results

Our implementation review found that GSA IT did not fully implement 4 of the 47 action steps in its action plan. Specifically, GSA IT did not:

- Complete three action steps requiring Google Sites owners to sign a memorandum of understanding (MOU) accepting responsibility for the proper operation of their site. This requirement only applied to site owners who wished to continue allowing GSA-wide access to their site.
- Fully implement an action step to notify affected individuals for whom the Agency identified a moderate or high risk of potential harm based on the PII involved.

Upon completion of our testing, we discussed our preliminary findings with Agency management. In response to our findings, GSA developed and issued an instructional letter to its employees related to the management of its Google Sites. We found the instructional letter to be responsive to the recommendation; therefore, no further action is needed related to this recommendation. Additionally, the Agency enlisted a third-party source to assist with its efforts to locate the remaining 14 moderate and high risk individuals. While the Agency was able to notify 6 out of 14 individuals, it must decide whether or not to pursue other means for locating and communicating with the remaining 8 individuals. A revised action plan addressing these open action steps must be submitted within 30 days to the GAO/IG Audit Management Division.

Finding 1 – GSA could not provide signed MOUs to support that Google Sites owners accepted responsibility for operating and managing their sites.

For the management of Google Sites, the corrective action plan states that users must sign an MOU to accept responsibility for the proper operation of their Site. The corrective action to be taken applied to action steps in Recommendations 1, 3, and 5. However, GSA could not provide signed MOUs to support that Google Sites owners accepted responsibility for operating and managing their sites in accordance with federal and GSA regulations and standards.

Google Sites is a tool available to GSA employees to facilitate collaborative processes within the Agency. Sites are not intended to be used as intranet platforms that are accessible GSA-wide; however, exceptions may be granted by the Office of Communications and Marketing (OCM) and GSA IT. OCM and GSA IT developed an MOU template, in response to our recommendations, to ensure that Google Sites approved to share information GSA-wide are operated in a manner that mitigates or reduces known risks. The action plan required OCM, GSA IT, and the organization/owner operating the Google Site to sign the MOUs.

After obtaining an inventory of 24 Google Sites shared GSA-wide in its cloud computing environment, we requested the MOU for 5 randomly selected sites. In response, GSA IT provided an email from OCM stating that an OCM Associate Administrator decided to issue an instructional letter instead of having individual MOUs signed. However, the

corrective action plan was never updated to reflect this change. We were unable to locate the instructional letter on the Agency's intranet and neither GSA IT nor OCM provided the instructional letter by the completion of our testing on May 3, 2016.

Subsequent to the completion of our testing, GSA's Chief Information Officer and the Associate Administrator of the Office of Communications and Marketing signed Instructional Letter OCM IL-16-01, *GSA Google Sites*, on May 18, 2016. Although the corrective action plan did not include the development of an instructional letter, based upon our review, the instructional letter contains sufficient language regarding the roles, responsibilities, and management of sites by owners and the services and staff offices. Specifically, the instructional letter, like the MOU, (1) promulgates criteria to ensure that site owners are aware of the requirements for safeguarding PII in GSA's cloud computing environment and (2) formally establishes policies to determine which sites are non-compliant. Therefore, the instructional letter has the same intended effect as the MOU as one of several internal control activities responsive to Recommendations 1, 3, and 5. Accordingly, no further action is needed.

Finding 2 – GSA could not provide evidence to prove that it had performed the actions it outlined to notify individuals identified as being at high or moderate risk for identity theft.

GSA did not provide evidence that it performed the actions outlined in its plan for notifying the remaining individuals affected by the PII breach in August 2014. GSA originally identified 907 individuals affected by the breach. The Agency notified 729 of these individuals but initially could not locate the other 178. Collaboration between the Office of the Chief Information Security Officer (OCISO), Senior Agency Official for Privacy (SAOP), and program staff reduced the number of affected individuals that had not been notified to 47. GSA then established risk ratings based on the type of PII exposed and the potential for harm to the individual, such as identity theft. After assigning a risk rating to the outstanding individuals, GSA determined that it would continue its efforts to notify those 14 individuals rated high and moderate risk. See *Figure 1* for the criteria of each risk rating.

Figure 1 - Risk Rating Criteria

Risk Rating	Identifiers for Risk of Harm
High	Social Security Number, Name with Last 4 Digits of Social Security Number
Moderate	Name with Date of Birth or Passport Number
Low	Name, Meal Preference, Home Phone Number, Religion

GSA outlined its efforts to obtain contact information for those remaining individuals in a plan for identifying actions to be taken for individuals where the risk for identity theft is high or moderate. Specifically, GSA stated that it would work with the Office of

Personnel Management, review the National Change of Address database, and use commercial products (*e.g.*, skip tracing or similar service).[1] We requested supporting evidence related to these actions. However, GSA was not able to provide evidence that it had actually performed the actions it outlined.

Upon completion of our testing, GSA management enlisted a third-party source in an attempt to locate the contact information for the remaining 14 moderate or high risk individuals. As a result of this effort, GSA obtained contact information for 6 out of the 14 individuals. The Agency provided documentation showing that all 6 of these individuals were contacted via first class mail. For the remaining 8 individuals, the search results did not provide GSA with an acceptable level of confidence to attempt to contact them. Therefore, the Agency should determine whether it will take additional action to locate and communicate with these individuals. As such, the Agency should submit a revised action plan to address this open action step within 30 days to the GAO/IG Audit Management Division.

[1] Skip tracing is the process of locating a person's whereabouts for any number of purposes.

Conclusion

Our implementation review found that GSA IT did not fully implement 4 of the 47 action steps in its action plan. However, after the completion of our review, GSA partially addressed the open action steps that were not fully implemented. Specifically, the Agency developed and issued an instructional letter related to the management of its Google Sites. We found the instructional letter to be responsive to the recommendation; therefore, no further action is needed. Additionally, the Agency was able to locate and notify 6 out of the 14 remaining individuals whose PII was rated at a moderate or high risk. However, the Agency still must decide whether it will continue to pursue the remaining 8 moderate or high risk individuals.

As a result of our findings, GSA must submit a revised action plan addressing this open action step within 30 days to this office and the GAO/IG Audit Management Division.

Audit Team

This review was managed out of the Acquisition and Information Technology Audit Office and conducted by the individuals listed below:

Sonya D. Panzo	Audit Manager
Felicia M. Silver	Auditor-In-Charge
Reynaldo M. Gonzales	Auditor

Appendix A – Report Distribution

Chief Information Officer (I)

Chief Privacy Officer (IS)

Associate Administrator, Office of Communications and Marketing (Z)

Branch Chief, GAO/IG Audit Management Branch (H1G)

Audit Liaison, GSA IT (IEB)

Assistant Inspector General for Auditing (JA)

Assistant Inspector General for Investigations (JI)

Director, Audit Planning, Policy, and Operations Staff (JAO)