

Personally Identifiable Information Unprotected in
GSA's Cloud Computing Environment
Report Number A140157/O/R/F15002
January 29, 2015

This report is one of several related GSA OIG reports that address unprotected sensitive information in GSA's cloud computing environment. We did not make these reports public at the time we provided them to GSA management because of concerns that the reports presented information about then existing security vulnerabilities. Because these concerns no longer exist, we are now making all reports available publicly as of January 27, 2017. The release of this report does not imply that a new event has occurred.

We have redacted management's response included in ***Appendix C*** at GSA's request as the Agency has deemed this information to be sensitive.



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

Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment

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




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

DATE: January 29, 2015

TO: Sonny Hashmi
Chief Information Officer
Senior Agency Official for Privacy
Office of the Chief Information Officer (I)

Kim Mott
Chief Privacy Officer
Policy and Compliance Division
Office of the Chief Information Security Officer (ISP)

FROM: 
Marisa A. Roinestad
Associate Deputy Assistant Inspector General for Auditing
Program Audit Office (JA-R)

SUBJECT: Personally Identifiable Information Unprotected in GSA's Cloud
Computing Environment
Report Number A140157/O/R/F15002

We identified a data breach of sensitive but unclassified building information and personally identifiable information (PII) within the General Services Administration's (GSA) Google cloud computing environment.¹ The sensitive information was accessible to GSA employees and contractors without a valid need to know such information. We determined that GSA was not proactive in securing sensitive data in its Google cloud computing environment and has not taken a comprehensive approach to correct the problem.

We notified GSA of this issue on July 29, July 30, and August 7, 2014. On August 19, 2014, we issued an alert report on the unprotected sensitive but unclassified building information.² We are now reporting on the PII that we found within GSA's Google cloud computing environment.

¹ A data breach is defined as, "the unauthorized or unintentional exposure, disclosure, or loss of sensitive information."

² Alert Report: *Sensitive But Unclassified Building Information Unprotected in GSA's Cloud Computing Environment* (Report Number A140157/P/R/W14001, August 19, 2014).

GSA has approximately 3.8 million Google Docs, 12,000 Google Groups, and 6,000 Google Sites in its Google cloud computing environment.³ During our audit, we reviewed a limited number of these documents and found PII was accessible to those without a valid need to know the information. We do not know how many of the unreviewed documents in GSA's Google cloud computing environment contain unprotected sensitive content. Therefore, we offer no assurance that all instances of unprotected PII have been identified.

After we notified the Office of the Chief Information Officer (OCIO) of the documents we identified containing unprotected PII, it determined that 907 individuals were affected by the data breach. However, GSA has not assessed the full extent of unprotected PII in its Google cloud computing environment. For this assessment, GSA has identified potentially sensitive documents, but has yet to review the documents. The OCIO explained that a manual review of documents to determine their sensitivity is a time-consuming process requiring the involvement of multiple business lines. As of November 6, 2014, the OCIO had not begun this process but intended to begin a manual review in the future.

On August 18 and 20, 2014, GSA issued a breach notification to approximately 600 of the 907 individuals that GSA determined were affected by the data breach. The notification was non-descriptive and minimized the severity of the breach to those affected. Additionally, approximately 300 affected individuals had not received a breach notification, as of October 21, 2014.

Currently, GSA has only taken limited steps to secure sensitive information within its Google cloud computing environment. Over 3 months have elapsed since our initial notifications, and GSA has used only reactive, short-term solutions to protect sensitive information.

The OCIO initially restricted all Google Groups, Sites, and Docs that were available Agency-wide. Currently, the OCIO runs a program that restricts any Google Groups and Sites that have been reopened Agency-wide. As of September 24, 2014, the OCIO also implemented automated searches of all Google Docs to flag instances of potential PII using 47 keywords and two preset searches within the search tool.⁴ Of these keywords, 42 of the 47 were selected from the list of 80 we provided on August 7, 2014.⁵ Documents containing PII will not be flagged unless they contain one of the 47 keywords or are found by one of the preset searches. Further, if a document is in an image format, the automated search is not able to review the content of the document for sensitive information.

³ These applications allow users to store and access files as well as collaborate in online forums and email-based groups.

⁴ The program that the OCIO uses to implement automated searches has preset searches for social security numbers and credit card information.

⁵ The keywords that the audit team provided to the OCIO were developed during an ad hoc brainstorming session and should not be considered a complete inventory to identify all PII.

The automated searches only take action to restrict documents identified as shared Agency-wide. No action is taken on documents not shared Agency-wide, regardless of the number of individuals with access or their need to know the information. Furthermore, GSA has not evaluated the over 10,000 flagged documents to determine the sensitivity of the information.

Google Docs attached to emails within Google Groups or linked to webpages within Google Sites will be scanned by the automated search. The OCIO's automated searches do not scan the content of Google Groups or Sites. Therefore, emails and website content may contain PII, which remains unscanned.

GSA must take additional, thorough action to identify and remediate all instances of PII found in this environment.

See **Appendix A** – Purpose, Scope, and Methodology for additional details.

If you have any questions regarding this report, please contact me, Marisa A. Roinestad, Associate Deputy Assistant Inspector General for Auditing, at marisa.roinestad@gsaig.gov/202-273-7241 or any member of the audit team at the following:

Sonya D. Panzo	Audit Manager	sonya.panzo@gsaig.gov	(202) 273-7333
Robert Fleming	Auditor-In-Charge	robert.fleming@gsaig.gov	(202) 273-4995

On behalf of the audit team, I would like to thank you and your staff for your assistance during this audit.

Background

As part of the Office of Management and Budget's (OMB) Federal Cloud Computing Strategy, GSA was one of the first federal government agencies to adopt a cloud-based environment to host its Agency-wide email system and collaboration services. This transition provided GSA employees with access to collaboration tools including, but not limited to, Google Groups, Sites, and Docs. GSA awarded its cloud computing contract to Google on December 1, 2010, and launched its cloud computing environment Agency-wide in June 2011.

We identified access control weaknesses in GSA's Google cloud computing environment. By browsing GSA's Google Groups, Sites, and Docs applications, we were able to access PII, without having a valid need to know such information.⁶

*GSA Rules of Behavior for Handling Personally Identifiable Information (PII)*⁷ references OMB M-06-19⁸ for the definition of PII as:

...any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

GSA defines data breaches of PII as:

...the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic.⁹

⁶ The OIG previously reported on weaknesses in GSA's efforts to protect PII, prior to the implementation of GSA's Google cloud computing environment. *Improvements to the GSA Privacy Act Program Are Needed to Ensure that Personally Identifiable Information (PII) is Adequately Protected* (Report Number A060228/O/T/F08007, March 31, 2008), concluded that improved management controls were needed to ensure that PII was consistently protected and the risk of unauthorized or unintentional disclosure of privacy information was reduced. *FY 2008 Office of Inspector General FISMA Review of GSA's Information Technology Security Program* (Report Number A080081/O/T/F08016, September 11, 2008), concluded that GSA's breach notification policy did not address the timeliness of the notification of individuals affected by breaches and did not address who will notify affected individuals.

⁷ GSA Order HCO 2180.1, *GSA Rules of Behavior for Handling Personally Identifiable Information (PII)*, dated August 9, 2009, was the policy in place during our fieldwork. This order was replaced on October 29, 2014, by GSA Order CIO P 2180.1.

⁸ OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.

⁹ GSA Order CIO P 2180.1, *GSA Rules of Behavior for Handling Personally Identifiable Information*, dated October 29, 2014. The prior order, GSA Order HCO 2180.1, was in place during our fieldwork. The PII data breach included in this audit report qualified as a breach under both policies.

GSA Information Technology (IT) Security Policy emphasizes the principle of granting access to information only to individuals with a valid need to know the information.¹⁰ PII should only be stored on systems protected by adequate access controls to ensure that data is only made available to those with a valid need to know the information.

The objectives of our audit were to: evaluate the nature and types of 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.

Results in Brief

Our limited review of GSA's Google cloud computing environment, which contains approximately 3.8 million documents, disclosed personally identifiable information that was accessible to employees and contractors without a valid need to know the information. As a result, the OCIO determined that the PII of at least 907 government employees, contractors, and job applicants was accessible Agency-wide. Individuals whose PII was accessible may be at risk for identity theft, harassment, embarrassment, or potential prejudice. To date, the scope of the vulnerable data remains unknown because GSA has not determined the full extent of the data breach and has not attempted to identify other potentially affected individuals. Additionally, the 907 identified individuals may not be fully aware of the potential impact that the breach could cause because GSA's notifications did not include important details about the breach. GSA must perform a comprehensive assessment of the security and protection of sensitive information in its Google cloud computing environment.

Findings

Finding 1 – Personally identifiable information was accessible to employees and contractors without a valid need to know the information.

PII in GSA's Google cloud computing environment was, and still may be, accessible by people without a valid need to know the information. Over 3 months after we first alerted GSA to the vulnerability in its Google Groups, Sites, and Docs, the scope of that vulnerability and the extent to which PII has been exposed remains unknown. Prior to our review, GSA did not restrict access to documents containing PII in its Google cloud computing environment. This unrestricted access has placed the privacy of at least 907 government employees, contractors, and job applicants at risk. GSA has not taken sufficient action to determine the full extent of the data breach, which means that others may also be impacted.

¹⁰ GSA Order CIO P 2100.11, *GSA Information Technology (IT) Security Policy*, dated September 19, 2013.

At the time of our review, PII data in GSA's Google applications were accessible to all GSA employees and contractors, partially due to improper access settings. GSA's settings for Google Groups, Sites, and Docs allow access to all GSA employees and contractors with GSA email accounts, regardless of their need to know the information.¹¹ As such, it is the responsibility of the creator or owner of the Google Group, Site, or Doc to evaluate the data security needed and adjust the access settings accordingly. However, because this was not done, documents containing PII were accessible to GSA employees and contractors who did not have a valid need to know such information. As a result, the affected persons could be at risk for identity theft, harassment, embarrassment, inconvenience, unfairness, or potential prejudice. GSA has also incurred credit monitoring expenses for the affected individuals. Additionally, GSA might be found liable for not keeping medical information confidential if an aggrieved individual were to file a complaint with the Equal Employment Opportunity Commission alleging improper disclosure of medical information.¹²

Our limited queries in GSA's Google cloud computing environment found documents with PII for government employees, contractors, and job applicants that were accessible by employees and contractors who did not have a valid need to know the information. These documents included individuals' names, in conjunction with other unique identifying information, such as:

- **Social Security Numbers:** There were 36 instances of full or partial social security numbers found in four documents that included a job application and contractor payroll registers.
- **Medical and Dietary Needs:** There were 32 instances of special medical needs and 82 instances of special dietary needs found in a spreadsheet listing registrants for a 2011 GSA training and expo.
- **Passport and Driver's License Numbers:** There were three passport numbers and six driver's license numbers found in two emails regarding clearance and background investigations.
- **Birth Dates and Location:** There were ten instances of dates of birth, as well as one instance of a place of birth, found in a job application and two emails regarding clearance and background investigations.
- **Home Addresses:** There were 36 instances of home addresses found in four documents that included a resume and contractor payroll registers. Additionally,

¹¹ As of August 15, 2014, there were 11,701 federal employees and 4,237 contract employees with active GSA email accounts.

¹² In *Complainant v. Patrick R. Donahoe, Postmaster General, United States Postal Service (Western Area)*, EEOC DOC 0120133064 (November 1, 2013), the Equal Employment Opportunity Commission found that the United States Postal Service failed "to keep certain medical information of its employees confidential" by allowing said information to be "improperly accessed and available...to any employee with access...."

in a spreadsheet listing registrants for a GSA training and expo, most employees listed their work addresses; however, some employees listed personal addresses. We verified three instances of personal addresses in the spreadsheet, but we did not analyze the over 3,000 addresses.

- **Personal Email Addresses:** There were 231 personal email addresses found in a spreadsheet listing registrants for a 2011 GSA training and expo, a resume, and two contact lists.
- **Personal Telephone Numbers:** There were 520 personal home and cellular telephone numbers found in eight documents that included call lists, a job application, and a resume. Further, for 192 of the 520 telephone numbers, the employees specifically requested that the numbers be kept private.

GSA has yet to undertake a comprehensive assessment of its Google cloud computing environment to determine the full extent of the PII that was accessible. To date, GSA has taken only limited actions based on our original findings. For example, GSA has taken steps to secure the PII that we identified, initially restricted all Google Groups, Sites, and Docs that were available Agency-wide, and implemented automated searches of Google Docs using keywords provided by the GSA OIG. Additionally, GSA advised its employees to limit sharing to only those who need access and to avoid sharing information in Google Groups, Sites, and Docs with all GSA employees and contractors. Further, as of August 11, 2014, as a best practice, GSA has asked its employees not to enable the sharing selection "All organization members," although it remained the default setting when creating a Google Group.

However, these actions are limited and have not included an evaluation of the entire Google cloud computing environment. As a result, an unknown number of individuals may still be at risk. As of November 6, 2014, GSA has also not evaluated documents flagged by its automated searches as potentially containing PII to determine the sensitivity of the information identified and if the users with access have a valid need to know the information. Further, the automated search is not able to review the content of images for sensitive information. As a result, additional action is needed to ensure the security of PII.

Finding 2 – Breach notifications to affected individuals were inadequate.

In response to the PII that was at risk in its Google cloud computing environment, GSA issued a breach notification to those individuals whose sensitive information was exposed. However, GSA did not provide all of the required information in the breach notifications and, as of November 14, 2014, has not notified all of the affected persons.

For those individuals whose information was exposed and who had available contact information, GSA emailed a mass breach notification to the affected individuals on August 18 and 20, 2014, to inform them that a breach occurred and how they could

further protect their information. The following is an excerpt from the notification (see **Appendix B** for the complete notification):

I am contacting you regarding a data security incident that occurred at General Services Administration (GSA). This incident involved some of your personal information. Your information never went outside the GSA firewall and may have been viewed by GSA employees who have completed privacy training and understand the importance of protecting PII.

GSA takes this incident seriously and is committed to fully protecting customer information and assuring the security of your data. While we believe the risk of harm to you is low, it is always a good idea to monitor your credit.

This notification did not include details of the breach as required by OMB M-07-16¹³ and GSA Order HCO 9297.2B.¹⁴

- **Timeframe:** The timeframe that information was available to individuals who did not have a valid need to know the information. Some individuals' PII could have been at risk for over 3 years.
- **Date:** The date the breach was discovered.
- **Descriptive Information:** Descriptions of the types of PII, as identified in *Finding 1*, that were involved in the breach.
- **Investigative Actions:** How GSA is investigating the breach, mitigating losses, and protecting against further breaches.

The OCIO did not include descriptions of the exposed information in the notifications due to the many types of PII exposed. As identified in *Finding 1*, social security numbers, medical and dietary information, passport and driver's license numbers, birth data, home addresses, personal email addresses, and/or personal telephone numbers of affected individuals were accessible to those without a valid need to know the information. Without a comprehensive notification, affected individuals may not be fully aware of the identity theft, harassment, embarrassment, inconvenience, unfairness, or potential prejudice the breach could cause.¹⁵

In addition, the issued breach notification conveys a false sense of security to the affected individuals by stating that exposed information "never went outside the GSA firewall" (see notification in **Appendix B**). Though GSA may be able to confirm that external third-parties did not penetrate the GSA firewall to view sensitive information,

¹³OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

¹⁴GSA Order HCO 9297.2B, *GSA Information Breach Notification Policy*, dated March 24, 2011.

¹⁵Harms cited in OMB M-07-16.

GSA cannot ensure that PII did not leave the Agency. GSA cannot determine, with certainty, the number of times a document has been accessed or by whom, beyond a 180-day window.¹⁶ The possibility exists that individuals without a valid need to know the information may have saved sensitive information prior to the OCIO's implementation of access restrictions on GSA's Google Groups, Sites, and Docs. Given this, the Agency cannot determine whether internal users could have intentionally or unintentionally leaked sensitive information, including PII.

Further, as of October 21, 2014, approximately 300 individuals affected by the breach still had not received a notification. According to GSA, these individuals did not have complete or up-to-date contact information available. GSA should make every effort to alert the impacted individuals as soon as possible, as required by GSA Order HCO 9297.2B.

Conclusion

Protecting sensitive data is critical. Without the proper controls to ensure that PII is not available to, or accessible by, individuals who do not have a valid need to know the information, the Agency risks damaging its finances and reputation. GSA is taking actions to address the PII that we identified, but GSA needs to take further steps to identify and assess the full extent of the PII that remains at risk. Further, not all of the affected individuals have been notified about their exposed data; and those who did receive notices were not provided with a full description of the breach or a timeframe regarding the availability of the PII to individuals who did not have a valid need to know the information. Given the nature of these issues and the length of time from our original notification to the Agency, GSA needs to take immediate, comprehensive action to address the vulnerability of PII in its Google cloud computing environment.

Recommendations

We recommend 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.

¹⁶ The OCIO maintains an access log per document that can be used to determine the individuals who have viewed or modified each document in GSA's Google cloud computing environment within the last 180 days. The OCIO did not review the access logs for the documents we identified as containing PII.

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 OMB M-07-16.
8. Review and update GSA Order HCO 9297.2, as necessary. Ensure the policy incorporates a structured response time schedule for notifying affected individuals for all suspected and confirmed breaches.

Management Comments

In its comments, management took no exception to our audit findings and recommendations. Management's response outlines corrective actions that the Agency has taken and plans to take to address the recommendations included in this report (see **Appendix C**).

Appendix A – Purpose, Scope, and Methodology

Purpose

We initiated this audit in response to the GSA OIG Office of Forensic Auditing, Evaluation, and Analysis's discovery of unprotected sensitive information residing in GSA's Google cloud computing environment.

Scope and Methodology

We interviewed GSA system security officials to gain an understanding of the collaboration tools available within GSA's Google cloud computing environment and how the Agency uses these tools. We conducted search queries within GSA's Google Groups, Sites, and Docs applications, using keywords such as resume, social security number, and date of birth. We also used Intelligencer, a GSA nationwide search engine available to all employees within GSA. We collected documents containing PII that were available with our audit team's basic access privileges.

Our queries were not exhaustive and the information collected is not comprehensive. The examples cited in this report represent only a sample of the documents containing PII that we found. We do not know how many of the 3.8 million documents in GSA's Google cloud computing environment contain unprotected sensitive content. Therefore, we offer no assurance that all instances of unprotected PII have been identified.

Except as noted below, we conducted our audit between July and August 2014 in accordance with generally accepted government auditing standards.¹⁷ These 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

This audit was initiated because we identified specific issues needing immediate management attention. As a result, the planning for this audit was limited to the steps necessary to assess the issues identified in the *Findings* section of this report.

Internal Controls

We evaluated internal controls as they relate to our audit scope and objectives. We conducted a select review of management, operational, and technical controls implemented for GSA's Google cloud computing environment. The Findings and

¹⁷ On February 1, 2016, we added this paragraph and the following paragraph to ensure full compliance with generally accepted government auditing standards. All other information in the report, including the findings and recommendations, remains the same.

Recommendations sections of this report state in detail GSA's need to strengthen specific controls to increase the protection of PII.

Appendix B – Breach Notification to Affected Individuals

The following is the breach notification that GSA sent to the affected individuals:

From: **credit monitoring** <creditmonitoring@gsa.gov>

Date: Mon, Aug 18, 2014 at 3:52 PM

Subject: Important Message - Please Read

To:

I am contacting you regarding a data security incident that occurred at General Services Administration (GSA). This incident involved some of your personal information. Your information never went outside the GSA firewall and may have been viewed by GSA employees who have completed privacy training and understand the importance of protecting PII.

GSA takes this incident seriously and is committed to fully protecting customer information and assuring the security of your data. While we believe the risk of harm to you is low, it is always a good idea to monitor your credit.

We would like to offer GSA funded credit monitoring for a period of one year. We're in the process of setting this up now and will contact you in a subsequent email with information on how to set it up. Please know that every effort is made to protect your personal information. Steps have been taken to ensure this event does not reoccur. If you have any questions please feel free to contact me at creditmonitoring@gsa.gov.

Below are things you can do to protect yourself.

Monitor your financial account statements and immediately report any suspicious or unusual activity to your financial institution.

Request a free credit report at www.AnnualCreditReport.com or by calling [1-877-322-8228](tel:1-877-322-8228). It might take a few months for most signs of fraudulent accounts to appear on the credit report. Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus – Equifax, Experian, and TransUnion – for a total of three reports every year. The annual free credit report can be used by you to self-monitor for identity theft.

Equifax: [1-800-525-6285](tel:1-800-525-6285); www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: [1-800-680-7289](tel:1-800-680-7289); www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Review resources provided on the Federal Trade Commission (FTC) identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information on identity theft.

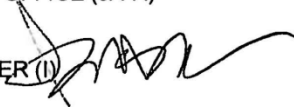
Appendix C – Management Comments



Office of the Chief Information Officer

January 15, 2015

MEMORANDUM FOR MARISA A. ROINESTAD
ASSOCIATE DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDITING PROGRAM AUDIT OFFICE (JA-R)

FROM: SONNY HASHMI
CHIEF INFORMATION OFFICER (I) 

SUBJECT: Personally Identifiable Information Unprotected in GSA's Cloud
Computing Environment
Report Number A14015/O/R

The Office of the Chief Information Officer (GSAIT) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report entitled *Personally Identifiable Information (PII) Unprotected in GSA's Cloud Computing Environment, Audit Report Number A140157/O/R*.

GSAIT agrees that protecting GSA's sensitive information is a very important responsibility that we take very seriously. We also recognize that GSA's mission is to assist other agencies in serving the public. As the world becomes more complex and interconnected it is of the utmost importance to balance the security needs with the needs to collaborate and better deliver value to the American people. It is no longer possible for individuals to solve complex problems on their own. Highly collaborative environments have shown to be the most productive and deliver the most value. GSAIT will outline its risk-based approach to securely operating inside the Google environment. We have over 3,000,000 documents, sites, and groups (combined) and over 15,000 users. Our risk-based approach combines technical tools, ongoing monitoring, and user training. This methodology will reduce risk to an acceptable level to operate. We recognize that every system with active users and transactions, and connectivity to other systems and processes always poses a level of residual risk. In this vein, while no practical mechanism exists to inspect and verify each document that exists within the GSA network environment, our planned approach as outlined below will significantly increase GSA's confidence in the security and privacy of documents managed within the Google Apps environment.

GSAIT would like to highlight subset of actions that GSA has taken to further secure Google Groups, Sites, and Docs. Future actions will be highlighted under the OIG's recommendations.

GSAIT Actions taken to date to secure Google Groups:

1. 
2. 

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Appendix C – Management Comments (cont.)

- 2 -

3. [REDACTED]

4. [REDACTED]
[REDACTED]

GSAIT Actions taken to date to secure Google Sites:

1. [REDACTED]

2. [REDACTED]
[REDACTED]

3. [REDACTED]
[REDACTED]

4. [REDACTED]
[REDACTED]

5. [REDACTED]
[REDACTED]

GSAIT Actions taken to date to secure Google Documents:

1. [REDACTED]
[REDACTED]
[REDACTED]

2. [REDACTED]
[REDACTED]

3. [REDACTED]
[REDACTED]

GSA's responses to the OIG's recommendations are provided in-line below:

The following outline GSA's planned approach to address the recommendations outlined by the OIG in the subject audit report

OIG recommended that GSAIT:

1. Restrict all content contained in GSA's cloud computing environment to the content's owner until:

Appendix C – Management Comments (cont.)

- 3 -

- 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.

To implement OIG's first recommendation, GSA will take the following approach:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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.

Appendix C – Management Comments (cont.)

- 4 -

To implement OIG's second recommendation, GSAIT will:

[REDACTED]

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.

To implement OIG's third recommendation, GSA will take the following approach:

[REDACTED]

[REDACTED]

4. Reevaluate and recertify, on a routine basis, the sensitivity, relevance, and accessibility of all content contained in GSA's cloud computing environment.

To implement OIG's fourth recommendation, GSA will take the following approach:

[REDACTED]

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.

To implement OIG's fifth recommendation, GSAIT will:

[REDACTED]

Appendix C – Management Comments (cont.)

- 5 -

[REDACTED]

[REDACTED]

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.

To implement OIG's sixth recommendation, GSAIT will implement the following risk-based approach:

- [REDACTED]
- [REDACTED]
- [REDACTED]

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 OMB M-07-16.

To implement OIG's seventh recommendation, GSAIT will:

[REDACTED]

8. Review and update GSA Order HCO 9297.2, as necessary. Ensure the policy incorporates a structured response time schedule for notifying affected individuals for all suspected and confirmed breaches.

To implement OIG's eighth recommendation, GSAIT will:

[REDACTED]

Appendix C – Management Comments (cont.)

- 6 -

GSAIT is prepared to assist OIG with any information that may be needed for its consideration of this report.

If you have any additional questions or concerns, please do not hesitate to contact me or Kim Mott, Chief Privacy Officer, on 202-208-1317.

cc: GAO/IG Audit Response Branch (HIC)

Appendix D – Report Distribution

Chief Information Officer (I)

Chief Privacy Officer (ISP)

Associate Administrator, Office of Communications and Marketing (Z)

Branch Chief, GAO/IG Audit Response Branch (H1C)

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)