Office of Inspections and Forensic Auditing
Office of Inspector General
U.S. General Services Administration

CLOSING MEMORANDUM: Unsecured Sensitive Information in GSA Google Environment

August 19, 2014
JEF14-026-000

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 from the attachments at GSA's request as the Agency has deemed this information to be sensitive.

U.S. General Services Administration
Office of Inspector General

August 19, 2014

MEMORANDUM FOR: SONNY HASHMI
CHIEF INFORMATION OFFICER (I)

FROM: PATRICIA D. SHEEHAN
DIRECTOR
OFFICE OF FORENSIC AUDITING, EVALUATION & ANALYSIS (JE)

SUBJECT: Closing Memorandum
Unsecured Sensitive Information in GSA Google Environment
JEF14-026-000

EXECUTIVE SUMMARY

GSA's internal collaborative working environment does not provide adequate protections to prevent improper disclosure of sensitive information. Based on limited testing conducted by the OIG, we are unable to provide any assurance that sensitive information is adequately protected in the internal GSA Google Apps environment.[1] Additionally, at this time there remains an unknown quantity of sensitive information that was accessible to approximately 17,000 users of GSA's Google applications, including information protected by the Privacy Act (5 U.S.C. § 552a) and Trade Secrets Act (18 U.S.C. § 1905), and other sensitive documents concerning the Continuity of Operations Plans (COOP), federal security, and law enforcement activities.

Due to the Agency's inadequate protections over sensitive information, the OIG Office of Forensic Auditing, Evaluation and Analysis (JE) has referred this matter to the OIG Office of Audits (JA) to further assess GSA's efforts to identify and remediate all instances of improper sensitive data access control vulnerabilities within GSA's Google environment.

WHAT WE FOUND

On July 29, 2014, JE identified sensitive information contained in a GSA Google Group, including information covered under the Privacy Act (5 U.S.C. § 552a). The information could be accessed by any user of GSA's Google Groups, to include GSA employees and contractors with GSA email addresses.

On July 30, we tested access controls for the GSA Google Group identified on July 29, and found that the Group was now secure from access by non-Group members. However, additional limited testing of GSA's Google Groups found three additional Groups with unprotected sensitive information, including information covered by the Privacy Act (5 U.S.C. § 552a) and the Trade Secrets Act (18 U.S.C. § 1905). The Privacy Act information included employee names and Social Security numbers, dates of birth, places of birth, citizenship status, Declarations for Federal Employment (OF 306), Credit Report Authorizations (GSA Form 3665), employment histories, and requests for Public Trust Position (GSA Form 3646). The Trade Secrets Act information included confidential and propriety contractor

[1] GSA Google Apps include Google Groups, Google Sites, Google Drive, and others.

information. Other examples of information included employee names, adjudications of background investigations, access eligibility, and security levels. JE also found over 6,000 documents pertaining to GSA Contract Board of Civilian Appeals (CBCA) business.

Over the next two weeks, JE, augmented JA, initiated a proactive targeted search of the GSA Google environment, and discovered additional sensitive information in GSA Google Groups and Sites.

The additional information discovered includes, but is not limited to: the draft National Security Staff Cyber Response Group Protocol, which was for White House situational awareness of cyber threats affecting national security, national economic security or national public health and safety; law enforcement sensitive information from the Department of Homeland Security about the Boston Bombing Massacre; personal medical information; attorney-client protected documents; courtroom drawings, including the location of judges' chambers; an assessment of a federal law enforcement building utility vulnerability; a specific GSA Child Care Center Security Reference Guide that showed physical vulnerabilities; GSA Vulnerability Assessment of Windows Subject to Explosive Blast Loads; and LAN diagrams and IP addresses for federal buildings.

In addition, we reviewed GSA's US-CERT submissions on this matter and found one revision contained an error and another was not sufficiently descriptive of the vulnerabilities discovered by the OIG. We requested corrections and the Agency submitted amendments.

WHAT WE DID TO NOTIFY GSA

On July 29, 2014, the OIG alerted the GSA Senior Agency Information Security Officer of the initial JE finding via memorandum (attached).

On July 30, we briefed the GSA Chief of Staff and Chief Information Officer (CIO), and the Acting Inspector General handed the Chief of Staff a memorandum to the Administrator alerting him to the vulnerabilities the OIG continued to find in the GSA Google Groups application and recommending GSA take all necessary action, to include shutting down relevant systems, to ensure sensitive information is protected until the system is properly assessed and secured (attached).

We also notified the Chief Counsel at the CBCA that we could access one of their GSA Google Groups. They promptly shut it down.

On August 7, we again briefed the GSA Chief of Staff, along with the CIO and CIO staff. The Acting Inspector General also issued a second memorandum to the Administrator, notifying the Agency of subsequent testing results, and advising that the actions taken to date have not mitigated the original problem, nor protected against the exposure of additional sensitive information contained in GSA's Google environment (attached). The Acting Inspector General also expressed OIG concerns regarding inadequate incident reporting to US-CERT, and we asked the CIO to alert his federal counterparts.

JA, accompanied by JE, apprised the GSA FISMA auditors, Brown and Company, of the GSA Google Apps vulnerabilities on both July 31 and August 14.

On August 14 we met with the GSA Privacy Officer and advised that the PII breach was not limited to the 508 individuals identified in the Agency US-CERT notification, but rather an unknown number of persons were affected. We also met on this date with the Deputy Administrator and the PBS Deputy Commissioner, alerting them to the persistent lack of security over sensitive information in GSA Google Apps, and advising them of the need to take immediate action to secure sensitive information, evaluate vulnerabilities, and notify the persons and GSA tenants who are impacted.

AGENCY STEPS
On July 29, 2014, the GSA incident response team isolated the GSA Google Group identified by the OIG and took corrective action immediately to set security permissions for authorized users only. The Agency proceeded to submit a timely US-CERT incident report on the matter.

During the following weeks GSA submitted seven revisions to the original report, to include needed corrections based on OIG review.

GSA also provided it's action plan on August 18, 2014 (attached).

CONCLUSION
Because of the ongoing GSA Google Apps vulnerabilities identified and reported by JE, this matter was referred to the OIG Office of Audits to review GSA's efforts to identify and remediate improperly disclosed information. The OIG initiated an audit on August 14, 2014, and notified the Agency.

Attachments

U.S. General Services Administration
Office of Inspector General

August 7, 2014

MEMORANDUM FOR: DANIEL TANGHERLINI
ADMINISTRATOR (A)

THRU: ROBERT ERICKSON
ACTING INSPECTOR GENERAL (J)

FROM: PATRICIA D. SHEEHAN
DIRECTOR
OFFICE OF FORENSIC AUDITING, EVALUATION & ANALYSIS (JE)

SUBJECT: Security Breach

On July 29, 2014, the OIG Office of Forensic Auditing, Evaluation & Analysis informed the agency that it had identified unprotected sensitive information contained in GSA's Google Groups, including information covered under the Privacy Act (5 U.S.C. § 552a) and the Trade Secrets Act (18 U.S.C. § 1905). The information was not secured and could be accessed by any user of GSA's Google Groups, to include GSA employees and contractors with GSA email addresses.

Since July 29, 2014, our office has conducted limited testing and discovered additional unprotected information in GSA Google Groups and Sites. This information includes, but is not limited to, courthouse plans, law enforcement sensitive information from the Department of Homeland Security about the Boston Bombing Massacre, personal medical information, and attorney-client protected documents.

The actions taken by GSA to date have not mitigated the original problem, nor protected the exposure of additional sensitive information contained in GSA's Google environment. We are increasingly concerned about the unknown amounts of sensitive information available to GSA employees and contractors without an official need to know. Furthermore, we are concerned that GSA's incident reports on this matter to U.S. CERT is inadequate. Enclosed is the inventory of our limited testing findings since the issuance of our memorandum on July 30, 2014.

We strongly reiterate our earlier recommendation that GSA take all necessary action, to include shutting down relevant systems, to ensure that all sensitive information is protected until the system is properly assessed and secured. We request detailed action plans and weekly briefings on how GSA intends to resolve this security breach.

Attachment

cc: Adam Neufeld
Chief of Staff (AC)

Sonny Hashmi
Chief Information Officer (I)

~~THIS MEMORANDUM AND ATTACHMENT CONTAIN SENSITIVE INFORMATION AND DISTRIBUTION IS RESTRICTED TO AGENCY OFFICIALS AND OTHER FEDERAL OFFICIALS WITH A NEED TO KNOW. PERSONS DISCLOSING THIS INFORMATION PUBLICLY OR TO OTHERS NOT HAVING AN OFFICIAL NEED TO KNOW ARE SUBJECT TO POSSIBLE ADMINISTRATIVE, CIVIL, OR CRIMINAL PENALTIES.~~

U.S. General Services Administration
Office of Inspector General

July 30, 2014

MEMORANDUM FOR: DANIEL TANGHERLINI
ADMINISTRATOR (A)

THRU: ROBERT ERICKSON *6*
ACTING INSPECTOR GENERAL (J)

FROM: PATRICIA D. SHEEHAN *6*
DIRECTOR
OFFICE OF FORENSIC AUDITING, EVALUATION & ANALYSIS (JE)

SUBJECT: Security Breach of GSA Google Groups Sensitive Information

On July 29, 2014, the OIG Office of Forensic Auditing, Evaluation & Analysis identified unprotected sensitive information contained in GSA's Google Groups, including information covered under the Privacy Act (5 U.S.C. § 552a) and the Trade Secrets Act (18 U.S.C. § 1905). The information was not secured and could be accessed by any user of GSA's Google Groups, to include GSA employees and contractors with GSA email addresses. Although we have only performed a limited assessment of the system since the problem was first discovered, to date we have identified thousands of documents in four separate "Google Groups" containing information that should have been protected.

The unprotected Privacy Act information included employee names and Social Security numbers, dates of birth, places of birth, citizenship status, Declarations for Federal Employment (OF 306), Credit Report Authorizations (GSA Form 3665), employment histories, and requests for Public Trust Position (GSA Form 3646). The unprotected Trade Secrets Act information included confidential and propriety contractor information. Other examples of unprotected information included employee names, adjudications of background investigation, access eligibility, and security levels.

While we alerted the GSA Senior Agency Information Security Officer yesterday of a single Google Group security breach, additional instances have been uncovered. We recommend GSA take all necessary action, to include shutting down relevant systems, to ensure sensitive information is protected until the system is properly assessed and secured.

U.S. General Services Administration
Office of Inspector General

July 29, 2014

MEMORANDUM FOR: KURT GARBARS
SENIOR AGENCY INFORMATION SECURITY OFFICER (IS)

THRU: LARRY LEE GREGG
ACTING DEPUTY INSPECTOR GENERAL (J)

FROM: PATRICIA D. SHEEHAN
DIRECTOR
OFFICE OF FORENSIC AUDITING, EVALUATION & ANALYSIS (JE)

SUBJECT: Agency Management Alert
JEF14-026-000

During the course of an ongoing evaluation, the OIG Office of Forensic Auditing, Evaluation & Analysis developed information regarding insufficient access controls over the handling of personally identifiable information (PII) contained in GSA's Google Group, "CPW Inquiry Security Packages". Primarily, any user of GSA's Google Groups could have accessed up to 405 records containing employee PII.

Examples of insufficiently protected PII include employee's full name and associated social security number, date of birth, place of birth, citizenship status, Declaration for Federal Employment (OF 306), Credit Report Authorization (GSA Form 3665), employment history, and request for Public Trust Position (GSA Form 3646).

We request that a written response detailing action taken be returned within 30 days from the date of this memorandum. If no final action has been taken with 30 days, please inform us of the status within 30 days and then provide an update each 30 days thereafter, with a completed response returned to us promptly when final action has been taken. The written response will be considered for further OIG review as appropriate.