Sensitive But Unclassified Building Information Unprotected in GSA's Cloud Computing Environment

Report Number A140157/P/R/W14001
August 19, 2014

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.

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

ALERT REPORT
Sensitive But Unclassified Building Information Unprotected in GSA's Cloud Computing Environment

Audit Number A140157/P/R/W14001
August 19, 2014

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

DATE: August 19, 2014

TO: Norman Dong
Commissioner
Public Buildings Service (P)

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

SUBJECT: Alert Report: Sensitive But Unclassified Building Information
Unprotected in GSA's Cloud Computing Environment
Report Number A140157/P/R/W14001

The purpose of this report is to alert the PBS to instances of unprotected sensitive but unclassified building information, as defined by GSA Order PBS 3490.1A, *Document Security for Sensitive but Unclassified Building Information,* that were uncovered by the Office of Inspector General. We recommend immediate corrective action be taken to secure all sensitive but unclassified building information that exists in GSA's Google cloud computing environment. Please forward an action plan addressing the recommendations to this office no later than September 3, 2014.

If you have any questions regarding this report or the ongoing audit, please contact me or members of the audit team at the following:

Marisa A. Roinestad	Associate Deputy Assistant Inspector General for Auditing	marisa.roinestad@gsaig.gov	202-273-7241
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 as we continue this audit.

Purpose and Objective

We initiated an audit in response to the Office of Inspector General (OIG) Office of Forensic Auditing, Evaluation, and Analysis's discovery of unprotected sensitive information residing in GSA's Google cloud computing environment. The objective of the audit is to determine if GSA has identified and remedied all instances of sensitive data access control vulnerabilities within GSA's Google cloud computing environment, as well as determine how to prevent additional instances in the future. While the audit is not yet completed, we are issuing this alert report due to the serious nature of the conditions we have identified.

Background

As part of the Office of Management and Budget's Federal Cloud Computing Strategy, GSA was one of the first agencies to adopt a cloud computing environment. GSA uses various Google applications, including Google Groups, Google Sites, and Google Docs as tools to foster a collaborative environment. GSA awarded the cloud computing contract on December 1, 2010, to host the agency-wide email, address book, calendar, and instant messaging system. The Google cloud computing environment launched GSA-wide in June of 2011.

On July 29, July 30, and August 7, 2014, senior OIG officials notified and provided GSA officials with numerous examples of unprotected sensitive information within GSA's Google cloud computing environment. The sensitive but unclassified building information was accessible to GSA employees and contractors without a valid need to know, which is the standard required by GSA policy. In spite of the previous notifications, as of August 14, 2014, unprotected sensitive but unclassified building information was still accessible. On that date, we verbally presented the findings and examples cited in this alert report to the GSA Deputy Administrator and the Deputy Commissioner, Public Buildings Service.

Weaknesses in PBS's efforts to protect sensitive but unclassified building information have been reported prior to the implementation of GSA's Google cloud computing environment. On September 30, 2008, an OIG audit[1] concluded that PBS needed to improve its implementation of existing controls over sensitive but unclassified building information to reduce the risk of inappropriate disclosure that may result in harm to people or property. The audit also found the oversight practices of PBS project managers and contracting officers regarding PBS security policies were inconsistent, and few of the PBS staff interviewed had received formal training on the sensitive but unclassified handling requirements and how to implement them. The OIG

[1] *Audit of PBS's Controls over Security of Building Information*, Report Number A070216/P/R/R08005. Subsequently, on March 31, 2010, the OIG issued the *Audit of PBS's Controls over Security of Building Information in Online Environments,* Report Number A070216/P/R/R10003. In this report, the OIG concluded that PBS needs to strengthen its controls over sensitive but unclassified building information specifically in online environments to reduce the risk of inappropriate disclosure of information that may result in harm to people or property.

recommended that PBS take steps to ensure that controls were in place to properly protect sensitive building information, train PBS officials on handling requirements, and implement a system of controls to ensure that GSA Order PBS 3490.1[2] requirements were followed by PBS project teams.

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 the tools. We conducted search queries within GSA's Google Groups, Sites, and Docs applications, using keywords such as confidential, court, and security. We also used Intelligencer, a search engine available to all employees within GSA. We collected sensitive but unclassified building documents 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 unprotected sensitive but unclassified building documents we found. We do not know the number and content of documents that are contained in GSA's nearly 12,000 Google Groups and 6,000 Google Sites, nor in the unquantified number of Google Docs. Therefore, we offer no assurance that all instances of unprotected sensitive but unclassified building information have been identified by the OIG.

Except as noted below, we conducted our audit between July and August 2014 in accordance with generally accepted government auditing standards.[3] 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 objective. 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. Additionally, the views of responsible officials were not obtained in writing and, as a result, were not included in this alert report.

Results in Brief

Sensitive but unclassified building information was accessible to GSA employees and contractors without a need to know the information. Further, sensitive but unclassified building information was not properly labeled.

[2] GSA Order PBS 3490.1, Document Security for Sensitive but Unclassified Paper and Electronic Building Information, is the predecessor policy to GSA Order PBS 3490.1A.

[3] On December 15, 2015, 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, except as noted in footnote 5.

Findings

Finding 1 – Sensitive but unclassified building information was accessible to employees and contractors without a need to know the information.

The safety and security of building tenants and government property is put at risk when sensitive but unclassified building information is accessible to individuals without a need to know such information. GSA has not implemented sufficient controls over its Google cloud computing environment. As a result, sensitive but unclassified building information is available to GSA employees and contractors,[4] regardless of their need to know the information. Per GSA Order PBS 3490.1A, *Document Security for Sensitive but Unclassified Building Information*:

- Access to sensitive but unclassified building information must be strictly controlled and limited to individuals with a need to know such information;
- Dissemination of sensitive but unclassified building information must only be to authorized recipients who have a need to know such information; and
- Access to and dissemination of sensitive but unclassified building information must be monitored via adequate controls.

Additionally, the policy states, “the more open the forum, the more generic or conceptual the information disseminated must be.”

Unprotected sensitive but unclassified building information found in GSA’s Google cloud computing environment that we discovered included:

- Child care centers: Occupant emergency plans outlined duress button locations, an account number for a regional Federal Protective Service MegaCenter, and evacuation routes.
- Courthouses: A detailed vulnerability assessment contained explosive blast loads as well as tenant locations and judges’ chambers throughout the building, and a blueprint indicating the location of judges’ chambers.
- Water sources: A Federal Bureau of Investigation pre-lease building security plan disclosed sensitive information about a building’s water supply.
- Building automation systems: Schematics related to GSALink contained the Internet Protocol addresses and physical locations of system components.
- Security and fire alarm systems: Security and mail screening procedures for a National Nuclear Security Administration campus, and an alarm layout for a federal building and courthouse.[5]

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

[5] This sentence includes an edit to the building description. The edit does not affect the audit finding.

Finding 2 – Sensitive but unclassified building information was not properly labeled.

Sensitive building documents are not properly marked to disclose whether or not the documents contained sensitive but unclassified information. Therefore, individuals may be unaware they are handling sensitive building information. GSA Order PBS 3490.1A, *Document Security for Sensitive but Unclassified Building Information,* requires PBS project team members to mark sensitive but unclassified building information as such. PBS project team members are not consistently implementing this policy.

Improperly labeled sensitive but unclassified building information found in GSA's Google cloud computing environment that we discovered included:

- Locations of secure functions or space: A courthouse floor plan showed the location of a courtroom and judges' chambers. Additionally, riser diagrams[6] and a building site readiness assessment questionnaire showed the locations and Internet Protocol addresses of building automation system components. These documents contained no markings indicating the sensitive nature of the material.
- Locations and types of structural framing and information regarding structural analysis: A detailed vulnerability assessment contained explosive blast loads as well as tenant locations and judges' chambers throughout the building. This document was insufficiently labeled, as it excluded the sensitive but unclassified designation.
- Information regarding security systems or strategies: A National Nuclear Security Administration campus security incident procedure and building operations plan identified locations of guard posts and security response protocols. Additionally, a building asset inventory identified the locations of guard offices and posts. These documents contained no markings indicating the sensitive nature of the material.

Recommendations

1. Evaluate all PBS content contained in GSA's Google cloud computing environment and immediately restrict any information that is available to those without a valid need to know the information.
2. Notify Government agencies, contractors, employees, and any other parties that were affected by the potential improper disclosure of sensitive but unclassified building information, unless it is determined that such notification is not warranted.
3. Prohibit the posting of any new PBS content to Google applications, including Google Groups, Google Sites, and Google Docs until sufficient controls are

[6] A riser diagram shows the major items of electrical equipment in a building.

established and implemented to ensure that sensitive but unclassified building information is properly protected and only accessible to individuals with a need to know such information.

4. Ensure PBS project team members mark sensitive but unclassified building information in accordance with GSA Order PBS 3490.1A.
5. Review existing building documents in GSA's Google cloud computing environment for missing or improper labeling.
6. Train PBS employees and contractors on the requirements in GSA Order PBS 3490.1A; specifically, how to handle sensitive but unclassified building information, and how to apply the concept of need to know. Ensure this training is mandatory and delivered on a routine basis.