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

Alert Memorandum: Sensitive Information Exposed in GSA's Google Groups

Memorandum Number A260019
October 14, 2025

October 14, 2025

TO: MICHAEL J. RIGAS
ACTING ADMINISTRATOR (A)

FROM: ROLANDO GOCO Digitally signed by ROLANDO GOCO Date: 2025.10.14 11:38:53 -04'00'
for ROBERT C. ERICKSON, JR.
DEPUTY INSPECTOR GENERAL (JD)

SUBJECT: Sensitive Information Exposed in GSA's Google Groups
Memorandum Number A260019

The purpose of this memorandum is to notify you of an issue that warrants your immediate attention. During the initial phase of our *Audit of GSA's Use of Acquisition Flexibilities*, we found documents and correspondence on GSA's Google Groups that contain sensitive information. Because these documents are accessible by all users with GSA email accounts, the sensitive information is exposed to users who do not have a legitimate business need to know.

BACKGROUND

GSA uses Google Workspace to collaborate across its organization. GSA's implementation of Google Workspace consists of productivity applications including Google's Gmail, Calendar, Groups, Meet, and Drive. Google Groups is a tool that allows GSA users to share information with multiple people at one time, learn about topics and join discussions, organize meetings and events, and use a collaborative inbox to assign conversations to members for tracking.

GSA's guidance on securely sharing through Google Workspace reminds users that "it's important to know what you're sharing and who has access to it."[1] The guidance further provides that users should "share only with those who have a business need to know." Accordingly, the guidance notes that users should "avoid sharing with 'all GSA' or 'anyone with the link.'" This guidance is reinforced through GSA's annual Information Technology Security and Privacy Awareness Training, which must be taken to receive and maintain access to GSA information technology systems.

[1] This guidance is available on GSA's "Sharing securely" intranet webpage.

GSA has also issued policy and guidance that address how different types of sensitive information should be handled in Google Workspace applications. For example, GSA has established policy and guidance for Controlled Unclassified Information (CUI), which the Agency defines as "unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or Government-wide policy."[2] The *GSA Controlled Unclassified Information (CUI) Program Guide* notes that information sharing should be limited to those with a lawful government purpose. Additionally, GSA's *Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property* requires CUI building information to be restricted to only those recipients who have a legitimate business need to know.[3]

RESULTS

Documents and correspondence containing sensitive information are exposed in GSA's Google Groups to users with GSA email accounts who do not have a legitimate business need to know. Examples include:[4]

- A GSA memorandum, marked as CUI, issued to U.S. Army personnel discussing unclassified [redacted] operations.[5] The memorandum also contains procurement-sensitive information, including estimated costs for [redacted].

- GSA documentation, marked as CUI, outlining the potential impact of the [redacted] on GSA operations. This document details recent incidents, threats, key actors, and upcoming dates of concern. It also includes recommendations for GSA personnel and facilities to mitigate the effects of possible attacks.

- U.S. Air Force correspondence, marked as CUI, detailing procurement cost and configuration data for government-furnished equipment.

- Defense Contract Audit Agency correspondence and an audit report marked as CUI. This report includes audit findings and proprietary information for a U.S. Department of Defense contractor.

[2] GSA Order 2103.2 CIO, *Controlled Unclassified Information (CUI) Policy* (April 10, 2021).

[3] GSA Order PBS 3490.3 CHGE 1, *Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property* (March 22, 2021).

[4] Due to the sensitivity of the exposed information identified, we notified GSA officials of our preliminary findings on October 7, 2025. That same day, GSA initiated actions to assess our preliminary findings. On October 8, 2025, we provided detailed information on our methodology and what we found to GSA IT officials for use in the Agency's corrective actions.

[5] Redactions represent CUI and other sensitive information.

- GSA documentation, marked as CUI, including cybersecurity risk assessments of some government contractors.

- Documents marked as For Official Use Only, including:

  - A Federal Emergency Management Agency document, [redacted].

  - A federal law enforcement Joint Intelligence Bulletin, [redacted]

- Personally identifiable information, including complete social security numbers of [redacted] federal employees performing work for [redacted].

The CUI and other sensitive data described above must be properly secured to protect against potential misuse, including physical security risks and financial harm.

CONCLUSION

Sensitive information is exposed in GSA's Google Groups to all users with a GSA email address who do not have a legitimate business need to know. The volume of sensitive information identified during our limited testing indicates that additional sensitive information may be exposed in GSA's Google Groups. Therefore, it is critical that the Agency ensures the proper management and maintenance of sensitive information stored in its Google Groups. GSA should also take appropriate measures to identify and notify those potentially affected by the exposed information in accordance with GSA's information breach policy.[6]

Furthermore, the exposure of sensitive information described in this alert memorandum is consistent with a recent incident identified by our office. In April 2025, we alerted GSA to the exposure of CUI and other sensitive information in GSA's Google Drive to GSA users who did not have a legitimate business need to know.[7] The recurring nature of these incidents demonstrates that additional management attention and oversight is needed to ensure that GSA properly protects sensitive information across its Google Workspace environment.

Compliance Statement

This alert memorandum complies with the GSA Office of Inspector General's established quality standards and internal controls. Any related audit, when completed, will comply with generally accepted government auditing standards.

[6] GSA Order CIO 9297.2C CHGE 1, *GSA Information Breach Notification Policy* (March 27, 2019).

[7] *Alert Memorandum: Sensitive Information Exposed in GSA's Google Drive* (Memorandum Number A250043-2, April 18, 2025).

Memorandum Distribution

Acting GSA Administrator (A)

Chief Financial Officer (B)

Acting Deputy Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Chief Information Officer (I)

Chief of Staff (I)

Assistant Inspector General for Auditing (JA)

Deputy Assistant Inspector General for Acquisition Audits (JA)

Deputy Assistant Inspector General for Real Property Audits (JA)

Director (JAO)

CONTACT US

For more information about the GSA OIG, please visit us online at www.gsaig.gov.

Office of Inspector General
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405
Email: oig_publicaffairs@gsaig.gov
Phone: (202) 501-0450 (General)
(202) 273-7320 (Press Inquiries)

GSA OIG Hotline
To report allegations of fraud, waste, abuse, mismanagement, or misrepresentations affiliated with GSA, please submit information to our hotline, www.gsaig.gov/hotline, or call (800) 424-5210.

Follow us:

gsa-oig

gsa_oig

@gsa-oig

gsa-oig