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

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

Memorandum Number A250043-2
April 18, 2025

April 18, 2025

TO: STEPHEN EHIKIAN
ACTING ADMINISTRATOR
GENERAL SERVICES ADMINISTRATION (A)

FROM: ROBERT C. ERICKSON, JR.
DEPUTY INSEPCTOR GENERAL (J)

ROBERT ERICKSON
Digitally signed by ROBERT ERICKSON
Date: 2025.04.18 10:00:49 -04'00'

SUBJECT: Sensitive Information Exposed in GSA's Google Drive
Memorandum Number A250043-2

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 Security Controls for GSA's Google Shared Drives*, we found documents on GSA's Google Drive that contain sensitive information. Because these documents are accessible by all GSA Google Drive users, including contractors, 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 enterprise. GSA's implementation of Google Workspace consists of productivity applications including Google's Gmail, Calendar, Groups, Meet, and Drive. Google Drive is a tool that allows all GSA users to store, share, collaborate, and access files from a mobile device, tablet, or computer.

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 addresses how different types of sensitive information should be handled in Google Drive. 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 access to CUI stored on Google Drive 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 containing sensitive information are exposed in GSA's Google Drive to GSA users, including contractors, who do not have a legitimate business need to know. Examples include:[4]

- **Safety Environmental Management Surveys for** [redacted][5] **–** Draft versions of these surveys are exposed to all GSA users. The surveys include detailed findings on the overall safety of the [redacted] Among other things, the surveys identify fire safety, occupational safety and health, and environmental conditions in the [redacted]. The surveys also include detailed blueprints of the [redacted]

- **Feasibility Study for a U.S. Courthouse –** A feasibility study to upgrade systems at the [redacted] is exposed to all GSA users. The study includes detailed blueprints that identify the locations of the [redacted] The blueprints also identify the locations of mechanical rooms, grand jury rooms, U.S. Marshals Service offices, and the courthouse's server room.

- **Controlled Unclassified Information –** Nine documents marked as CUI are exposed to all GSA users. For example, we found a site development plan for the [redacted]

[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 during our audit survey, we notified GSA officials of our preliminary findings on April 14, 2025. On April 15, 2025, GSA responded that they "take exposure [of] sensitive information seriously" and initiated corrective actions. We have provided detailed information on our findings to officials in the Office of GSA IT for use in the Agency's corrective actions.

[5] Redactions represent sensitive building and financial information.

[redacted] The plan includes information related to the building's fire protection, mechanical, electrical, and plumbing systems. It also includes ductwork requirements for the facility's sensitive compartmented information facilities. In another example, we found electrical drawings for the [redacted] The drawings detail the building's main electrical system, including the switchgear.

- **Vendor Financial Information –** Sensitive financial information is exposed to all GSA users for a vendor that [redacted] The exposed information includes an invoice containing the vendor's full bank account number and wire transfer information, as well as an Internal Revenue Service form with the vendor's tax identification number.

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 Drive to GSA employees and contractors 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 Drive. Therefore, it is critical that the Agency ensures the proper management and maintenance of sensitive information stored on its Google Drive. GSA should also take appropriate measures to identify and notify those affected by the exposed information in accordance with GSA's information breach policy.[6]

Compliance Statement

This alert memorandum complies with the Council of Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General. The related ongoing audit, when completed, will comply with generally accepted government auditing standards.

Audit Team

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

Sonya Panzo	Associate Deputy Assistant Inspector General for Auditing
Kyle Plum	Audit Manager
James Dean	Auditor-In-Charge
Yuanmei Liang	Auditor
Imani Foster-Wilson	Auditor

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

Memorandum Distribution

Acting GSA Administrator (A)

GSA Deputy Administrator (AD)

PBS Commissioner (P)

Chief Information Officer (I)

Deputy Chief Information Officer (ID)

Chief of Staff (I)

Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

Deputy Assistant Inspector General for Acquisition Audits (JA)

Deputy Assistant Inspector General for Real Property Audits (JA)

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