



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

Controlled Unclassified Information in GSA's Google Drive Was Improperly Exposed

Report Number A250043/I/T/F27002
October 27, 2026

Executive Summary

Controlled Unclassified Information in GSA's Google Drive Was Improperly Exposed

Report Number A250043/I/T/F27002

October 27, 2026

Why We Performed This Audit

GSA uses Google Workspace to collaborate across the Agency. GSA's implementation of Google Workspace includes Google Drive, which is a tool that allows all GSA users to store, share, collaborate, and access files from a mobile device, tablet, or computer.

According to GSA management, GSA users and contractors currently have 2.5 million documents stored in GSA's Google Drive. Some of these documents contain information that, while not classified, still requires some level of protection from unauthorized access by individuals who do not have a legitimate business need to know. This information is referred to as controlled unclassified information (CUI). Examples of CUI used by GSA include:

- **Physical Security Information** – Information related to the security of federal buildings, grounds, and property. This information includes floor plans and blueprints, as well as information on building security assessments, counterterrorism methods, and building automation systems.
- **Personally Identifiable Information** – Information that can be used to distinguish or trace an individual's identity. This information includes social security numbers, dates of birth, and home addresses.
- **General Proprietary Business Information** – Information related to a company's products, business operations, or activities. This includes information on a company's trade secrets, product research and development, existing and future product designs, and performance details.

In August 2014, we first reported that GSA did not protect sensitive information on child care centers, courthouses, water sources, building automation systems, and security and fire alarm systems in its Google cloud computing environment. We issued additional reports citing concerns regarding GSA's ability to protect sensitive information in its Google environment between 2015 and 2017.

In April 2025, we again identified unauthorized exposures of CUI in GSA's Google Drive. The exposed information included safety surveys for the [REDACTED] showing detailed blueprints of the [REDACTED]

██████████.¹ We also found a site development plan for the ██████████ ██████████ in Washington, D.C.; and a vendor's full bank account number and wire transfer information.

Because of its sensitivity, GSA must ensure that CUI stored in its Google Drive is properly protected against unauthorized exposure. Accordingly, we included this audit on our *Fiscal Year 2025 Audit Plan*. Our audit objective was to assess the effectiveness of security controls and privacy settings in place to protect the confidentiality, integrity, and availability of information stored within GSA's Google Drive as required by federal and Agency information technology security policies, procedures, standards, and guidance.

What We Found

GSA is not effectively protecting information stored within its Google Drive, resulting in unauthorized exposures of CUI. During a limited search of GSA's Google Drive, we found 116 files containing CUI that were improperly shared with all GSA users. As a result, the CUI was exposed to GSA employees and contractors who did not have a legitimate business need to know. The improperly exposed CUI included:

- **Physical Security Information** – Exposures of physical security information can create safety and security risks for building occupants. We found physical security information exposed in GSA's Google Drive, such as counterterrorism methods, continuity of operations plans, and blueprints showing access points to sensitive areas of federal buildings. Specific examples include:
 - Site plans for the ██████████ in Washington, D.C. The plans identify site entrances, badge holder and visitor routes, screening areas, and screening techniques.
 - A progressive collapse analysis for the ██████████, that describes the building's collapse vulnerabilities, defense vulnerabilities, and critical failure locations.
 - A presentation for the ██████████, that includes floor plans showing sensitive areas of the building. The sensitive areas shown in the floor plans include gun lockers, judges' chambers, jury rooms, metal detectors, and x-ray screening areas.
- **Personally Identifiable Information** – Exposures of personally identifiable information leave affected individuals vulnerable to identity theft, financial loss, embarrassment, and inconvenience. We found personally identifiable information exposed in GSA's

¹ Redactions in this report represent sensitive physical security, personally identifiable, and general proprietary business information.

Google Drive, including social security numbers, dates of birth, phone numbers, and addresses.

- **General Proprietary Business Information** – Exposures of general proprietary business information could reveal a company's trade secrets or business practices and be exploited by competitors. We found general proprietary business information exposed in GSA's Google Drive, including proprietary research and vendor proposals with technical and pricing information.

GSA did not detect that the CUI was exposed in its Google Drive because of deficiencies in its oversight. Specifically, GSA does not effectively manage its data loss prevention tool, which is a third-party software application used to prevent and detect CUI exposures. We found the following deficiencies in GSA's management of this tool:

- GSA has not fully completed annual reviews of the tool's search terms to ensure effective detection of CUI;
- Searches using the tool did not detect exposed documents that included current search terms;
- GSA did not incorporate many relevant terms from the Agency CUI guidance into the tool's search terms;
- GSA did not implement the available tool feature—optical character recognition—that could prevent some CUI exposures;
- GSA was unaware of the tool's file size limitation of 15 megabytes; and
- GSA did not document program decisions affecting CUI protection in Google Drive.

We also found that GSA lacks: (1) an approval process for properly sharing sensitive information and (2) a standard naming convention that could more effectively prevent exposures of CUI in GSA's Google Drive.

What We Recommend

We recommend that the GSA Chief Information Officer:

1. Restrict access for all 116 CUI documents exposed in GSA's Google Drive to only GSA users with a lawful government purpose to access that information.
2. Identify other CUI documents exposed to all GSA users not found during this audit and restrict these documents to only GSA users with a lawful government purpose to access that information.
3. Identify and notify the individuals affected by the exposed information in accordance with the *GSA Information Breach Notification Policy*.

4. Identify and implement additional controls to ensure that Agency employees only share CUI documents in GSA's Google Drive with users who have a lawful government purpose to access that information. At a minimum:
 - a. Implement an approval process for sharing CUI documents in Google Drive with all GSA users.
 - b. Develop a standard naming convention for CUI documents to more effectively identify and protect CUI in GSA's Google Drive.
 - c. Update Agency guidance and training materials to further emphasize the importance of CUI, the different categories of CUI, and how to appropriately flag CUI documents in Google Drive.
5. Improve management of the data loss prevention tool to better detect and prevent CUI exposures in GSA's Google Drive. Specifically, GSA's Security Operations & Engineering Division should:
 - a. Review, update, enforce, and document the process for the annual review of the data loss prevention tool's search terms.
 - b. Incorporate relevant terms from GSA's CUI guidance into the data loss prevention tool's search terms.
6. Assess and implement available enhancements to the data loss prevention tool to maximize detection and restriction of CUI exposures in GSA's Google Drive. The Security Operations & Engineering Division should:
 - a. Evaluate the current data loss prevention tool's optical character recognition feature for implementation.
 - b. Develop a process for evaluating new data loss prevention tool features for implementation.
 - c. Evaluate methods to identify exposed CUI documents larger than 15 megabytes and safeguard those documents.
7. Develop and implement a process to document and maintain management and operational decisions for the data loss prevention tool.

GSA's Chief Information Officer agreed with our recommendations. GSA's comments are included in their entirety in **Appendix E**.

Table of Contents

Introduction.....	1
Results.....	7
<i>Finding – GSA is not effectively protecting information stored within its Google Drive, resulting in unauthorized exposures of controlled unclassified information.</i>	<i>7</i>
Conclusion	17
Recommendations	17
GSA Comments.....	18
Appendix A – Objective, Scope, and Methodology.....	19
Appendix B – CUI Categories.....	21
Appendix C – List of 39 Terms Used to Search GSA’s Google Drive for Exposed CUI.....	22
Appendix D – List of 116 CUI Documents Exposed in GSA’s Google Drive to All Users.....	24
Appendix E – GSA Comments.....	31
Appendix F – Report Distribution	34

Introduction

We performed an audit of security controls and privacy settings for GSA's Google Drive.

Purpose

GSA must ensure that controlled unclassified information (CUI) stored in its Google Drive is properly protected against unauthorized exposure. Accordingly, we included this audit on the GSA Office of Inspector General's *Fiscal Year 2025 Audit Plan*.

Objective

Our audit objective was to assess the effectiveness of security controls and privacy settings in place to protect the confidentiality, integrity, and availability of information stored within GSA's Google Drive as required by federal and Agency information technology security policies, procedures, standards, and guidance.

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

Background

GSA uses Google Workspace to collaborate across the Agency. GSA's implementation of Google Workspace consists of collaboration 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. Google Drive consists of a private *My Drive* for each user; and many shared drives, which are owned by and accessible to teams. According to GSA management, GSA users and contractors currently have 2.5 million documents stored in GSA's Google Drive.

Some documents GSA uses to carry out its mission contain sensitive information, including CUI. Executive Order 13556, *Controlled Unclassified Information*, defines CUI as unclassified information "that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies."

CUI covers a broad range of sensitive information. Some categories of CUI are described below:

- **Physical Security Information** – Information related to federal buildings, grounds, and property that GSA owns or manages, including properties managed by other federal agencies on GSA's behalf. Examples of physical security information include information concerning building security assessments, counterterrorism methods, and automation systems.

- **Personally Identifiable Information (PII)** – Information that can be used to distinguish or trace an individual’s identity. Examples of PII include social security numbers, dates of birth, and home addresses.
- **General Proprietary Business Information** – Information related to a company’s products, business operations, or activities. Examples include financial information, trade secrets, product research and development, existing and future product designs, and company performance details.

See **Appendix B** for a complete list of the CUI categories we tested.

Safeguarding CUI

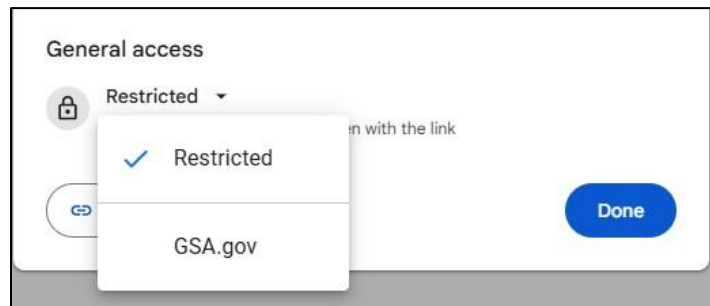
GSA must safeguard its CUI to protect against unauthorized disclosure. Executive Order 13556 established a program for managing CUI across the federal government. In accordance with this executive order, GSA implemented GSA Order CIO 2103.2, *Controlled Unclassified Information (CUI) Policy*, which requires CUI to be protected at all times to minimize the risk of unauthorized disclosure. GSA also included requirements for protecting CUI in GSA Order CIO 2100.1Q, *GSA Information Technology (IT) Security Policy*, which states that:

PII/CUI stored on network drives and/or in application databases must have proper access controls (i.e., user identification, authentication, and authorization) and shall be made available only to those individuals with a lawful government purpose.

The *GSA Controlled Unclassified Information (CUI) Program Guide* further instructs employees to limit access of CUI stored in GSA’s Google Drive to those with a lawful government purpose. Furthermore, GSA Order PBS [Public Buildings Service] 3490.3 CHGE 1, *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.

In an effort to protect CUI, GSA set the general access settings in its Google Drive to automatically restrict documents from access when they are uploaded unless a user manually selects the “GSA.gov” option. If the “GSA.gov” option is selected, the document can be shared with all GSA Google Drive users. *Figure 1* on the next page displays the general access settings for a document in Google Drive.

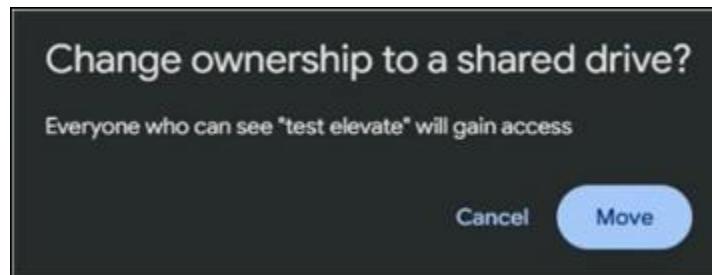
Figure 1. General Access Settings in GSA's Google Drive



GSA users can also upload documents to established Google shared drive folders. When users add documents to a Google shared drive folder that is already accessible to all GSA Google Drive users, the documents will inherit the folder's existing access settings.

Accordingly, a warning prompt automatically generates when a user attempts to add a document to a Google shared drive folder. This prompt notifies the user that moving the document will change the ownership to the shared drive setting. *Figure 2* below shows the prompt a user sees after trying to add a document to a Google shared drive folder named "test elevate."

Figure 2. Access Setting Inheritance Warning Prompt



Responsibility for GSA's Google Drive and Protection of CUI

The Office of GSA IT manages the operations and security of GSA's Google Drive. Specifically, GSA Google Workspace administrators within the Office of GSA IT monitor, troubleshoot, and configure all elements of GSA's Google Drive.

In addition, the Security Operations & Engineering Division (Security Operations Division), which is within the Office of GSA IT, is responsible for real-time security monitoring, threat detection and response, security architecture development, and automated security tools deployment to protect GSA's information systems and data assets. This division manages a third-party data loss prevention tool that GSA uses to protect against CUI exposures in GSA's Google Drive.

GSA employees who handle CUI content are responsible for ensuring that they properly maintain and store the documents to protect them from unauthorized release. According to GSA's *Controlled Unclassified Information (CUI) Policy*:

- (1) Everyone working in or with GSA who comes in contact with CUI is responsible for protecting and properly securing CUI, for reporting incidents, for following CUI policies and procedures, and for completing all required CUI training; and
- (2) Authorized holders who create CUI or manage applications containing CUI are responsible for ensuring the proper CUI markings are applied.

These requirements are reinforced in GSA's *2025 GSA IT Security and Privacy Awareness Training*. A portion of this training addresses the storage of sensitive information, such as CUI, in GSA's Google Drive. Specifically, the training reminds GSA users to:

Review Google Drive contents regularly: Remove people who no longer need access. Especially focus on docs [documents] that are shared GSA-wide (with or without links) to ensure no sensitive information might be shared with people who don't have a need to know.

Alert Report Issued in August 2014 Identified Exposed CUI

In August 2014, we reported that GSA did not implement sufficient controls over its Google cloud computing environment.² As a result, sensitive but unclassified building information was available to GSA employees and contractors, regardless of their need to know the information. This included sensitive information on child care centers, courthouses, water sources, building automation systems, and security and fire alarm systems.

GSA Implements a Data Loss Prevention Tool to Prevent and Detect CUI Exposures

In August 2014, in response to our audit report, GSA implemented a third-party data loss prevention tool in Google Drive that is designed to prevent and detect CUI exposures. GSA continues to use this application, and the Director of IT Audit and Records Management told us GSA has spent approximately \$7.8 million on it as of September 2026.

The data loss prevention tool searches documents shared GSA-wide in GSA's Google Drive for certain words or phrases related to CUI. If CUI is detected, the tool performs a pre-designed response, which could include restricting access to the document, flagging and informing the Security Operations Division, and sending an automated email to the document owner.

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

Audit Products Issued Between 2015 and 2017 Continued to Identify Unauthorized CUI Exposures and Deficiencies in GSA's Corrective Actions to Address the Audit Findings

After GSA implemented the third-party data loss prevention tool designed to prevent and detect CUI exposures, we continued to find problems. In January 2015, we reported that GSA did not restrict access to documents containing PII in its Google cloud computing environment, putting the privacy of at least 907 government employees, contractors, and job applicants at risk.³ The exposed PII included individuals' names in conjunction with other unique identifying information, such as:

- Social security numbers,
- Medical and dietary needs,
- Passport and driver's license numbers,
- Birth dates and locations,
- Home addresses,
- Personal email addresses, and
- Personal telephone numbers.

In January 2017, we issued reports on the corrective actions GSA took in response to our August 2014 and January 2015 audit reports.^{4,5} We found that GSA could not provide evidence that it notified individuals and other Agency points of contact that their information was improperly shared across GSA.

Alert Memorandums Issued in 2025 Continued to Identify Challenges in GSA's Protection of CUI from Unauthorized Exposure

During 2025, we again identified unauthorized exposures of CUI in GSA's Google Workspace. We notified GSA of these exposures through the following alert memorandums:

- In April 2025, we issued an alert memorandum on CUI exposures in GSA's Google Drive.⁶ We found that sensitive information was exposed in GSA's Google Drive to GSA employees and contractors who did not have a legitimate business need to know. This

³ *Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment* (Report Number A140157/O/R/F15002, January 29, 2015).

⁴ *Implementation Review of Action Plan: Sensitive But Unclassified Building Information Unprotected in GSA's Cloud Computing Environment, Report Number A140157/P/R/W14001, August 19, 2014* (Assignment Number A160096, January 26, 2017).

⁵ *Implementation Review of Action Plan: Personally Identifiable Information Unprotected in GSA's Cloud Computing Environment, Report Number A140157/O/R/F15002, January 29, 2015* (Assignment Number A160045, January 26, 2017).

⁶ *Alert Memorandum: Sensitive Information Exposed in GSA's Google Drive* (Memorandum Number A250043-2, April 18, 2025).

information included safety surveys for the [REDACTED] showing detailed blueprints of the [REDACTED]; a site development plan for the [REDACTED] in Washington, D.C.; and a vendor's full bank account number and wire transfer information.

- In October 2025, we issued an alert memorandum on CUI exposures in GSA's Google Groups.⁷ We found documents and correspondence containing sensitive information that were exposed in GSA's Google Groups to users who did not have a legitimate business need to know. This included CUI-marked documents containing estimated costs for [REDACTED] and detailed asset descriptions outlining aircraft capabilities, the potential impact of the [REDACTED] on GSA operations, and [REDACTED] correspondence detailing procurement cost and configuration data for government-furnished equipment.

⁷ Alert Memorandum: Sensitive Information Exposed in GSA's Google Groups (Memorandum Number A260019, October 14, 2025).

Results

Finding – GSA is not effectively protecting information stored within its Google Drive, resulting in unauthorized exposures of controlled unclassified information.

GSA is not effectively protecting information stored within its Google Drive, resulting in unauthorized exposures of CUI. During a limited search of GSA's Google Drive, we found 116 files containing CUI that were improperly shared with all GSA users. As a result, the CUI was exposed to GSA employees and contractors who did not have a legitimate business need to know. The improperly exposed CUI included:

- Physical security information, such as counterterrorism methods, continuity of operations plans, and blueprints showing access points to sensitive areas of federal buildings;
- Personally identifiable information, such as social security numbers and dates of birth; and
- General proprietary business information, such as proprietary research and vendor proposals with technical and pricing information.

GSA did not detect that the CUI was exposed in its Google Drive because of deficiencies in its oversight. Specifically, we found deficiencies in GSA's: (1) management of a third-party data loss prevention tool used to prevent and detect CUI exposures; and (2) policies, guidance, and procedures governing CUI.

CUI Was Improperly Exposed in GSA's Google Drive

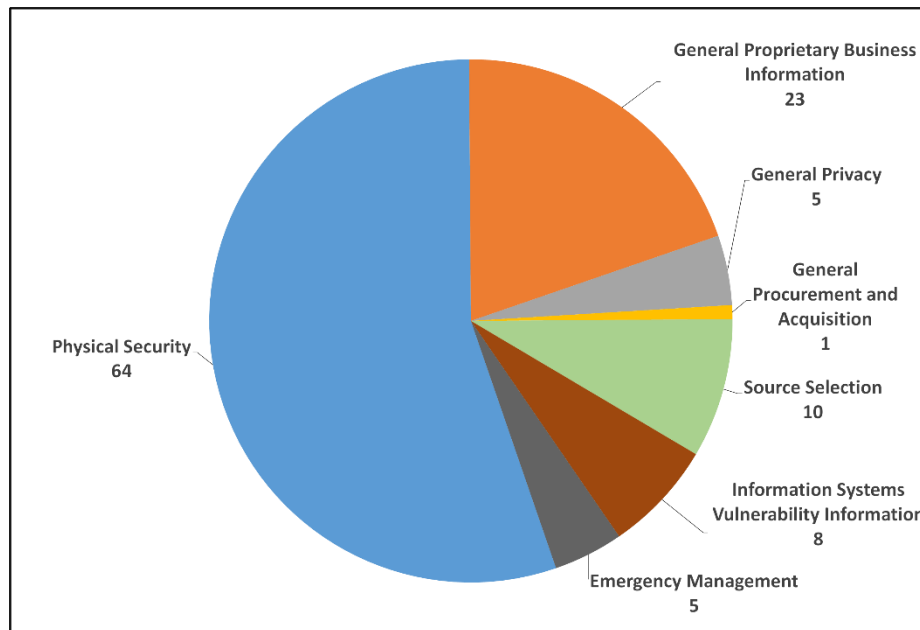
GSA's *Controlled Unclassified Information (CUI) Policy* requires all GSA employees to protect and properly secure CUI. The policy states that "CUI shall be protected at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders." It requires all CUI systems and information to be protected according to applicable laws, regulations, or government-wide policies.

GSA also established the *GSA Controlled Unclassified Information (CUI) Program Guide*, which further instructs employees to limit access of CUI stored in GSA's Google Drive to those with a lawful government purpose. A lawful government purpose is any activity or function that falls within the scope of the government's authorized legal authorities. GSA's "Sharing securely" intranet webpage states that users should "Avoid sharing with 'all GSA' or 'anyone with the link.'"

However, we found 116 CUI documents in GSA's Google Drive that were improperly shared with all GSA users. As a result, the CUI was exposed to GSA employees and contractors who did not have a legitimate business need to know. *Figure 3* on the next page includes a breakdown of the exposed CUI documents by CUI category. A list of the terms used in our search is

included in **Appendix C**, and a detailed listing of the exposed documents is included in **Appendix D**.

Figure 3. Exposed CUI Documents by CUI Category⁸



We provide specific examples of exposures of physical security information, PII, and general proprietary business information below.

Physical Security Information. At GSA, CUI includes physical security information related to federal buildings, grounds, and property that GSA owns or manages, including properties managed by other federal agencies on GSA’s behalf. Examples of physical security information include building security assessments, counterterrorism methods, and building automation systems.

Exposures of physical security information can create safety and security risks for building occupants. For example, site plans, blueprints, drawings, and progressive collapse analyses can be used by bad actors to identify and exploit security vulnerabilities.

Of the 116 exposed CUI documents we found during our limited testing, 64 (55.2 percent) contained physical security information. Specific examples of the exposed physical security CUI documents found during our audit include the following:

- **Site plans for the [REDACTED] in Washington, D.C.** – Identifies site entrances, badge holder and visitor routes, screening areas, and screening

⁸ We found CUI documents in seven of the nine CUI categories we tested for. See **Appendix B** for a complete list of the CUI categories we tested.

techniques. This document has the following marking: **“PROPERTY OF THE UNITED STATES GOVERNMENT. FOR OFFICIAL USE ONLY. Do not remove this notice. Properly destroy documents when no longer needed.”** (emphasis in the original)

- **Progressive collapse analysis for the [REDACTED]** – Describes the building’s collapse vulnerabilities, defense vulnerabilities, and critical failure locations. This document has the following marking: **“PROPERTY OF THE UNITED STATES GOVERNMENT COPYING, DISSEMINATION, OR DISTRIBUTION OF THESE DRAWINGS, PLANS, OR SPECIFICATIONS TO UNAUTHORIZED USERS IS PROHIBITED FOR OFFICIAL USE ONLY Do not remove this notice Properly destroy documents when no longer needed.”** (emphasis in the original)
- **U.S. Department of Defense presentation** – Identifies the security of a previous [REDACTED]. The presentation, which is dated 2012, includes a map of the [REDACTED]. It also includes a diagram of Washington, D.C., with [REDACTED]. This presentation has the following marking: **“UNCLASSIFIED//FOUO.”** (emphasis in the original)
- **Presentation for the [REDACTED]** – This presentation includes floor plans that show sensitive areas, such as gun lockers, judges’ chambers, jury rooms, metal detectors, and x-ray screening areas.
- **Continuity of operations plan for the [REDACTED]** – Outlines planning scenarios, including threats of massive explosion, civil disturbance, and weapons of mass destruction. This document has the following marking: **“FOR OFFICIAL USE ONLY (FOUO).”** (emphasis in the original)
- **Occupant emergency plan for the [REDACTED]** – Identifies the team’s office locations, evacuation assembly points, and assembly group leads. This plan also includes the safe haven locations for the child care center in the [REDACTED] in Washington, D.C.

Personally Identifiable Information. Personally identifiable information (PII) is categorized as general privacy information that can be used to distinguish or trace an individual’s identity. Examples of PII include social security numbers, dates of birth, and home addresses. PII exposures leave affected individuals vulnerable to identity theft, financial loss, embarrassment, and inconvenience. These exposures also leave GSA vulnerable to significant reputational risk and potential litigation.

We found PII exposures in five documents in GSA’s Google Drive. Although PII exposures only represent 4.3 percent of the CUI exposures found during our limited testing, these exposures could present significant risks to affected individuals and the Agency. Specific examples of the PII exposed in GSA’s Google Drive include the following:

- Federal employment paperwork for one person with full name, social security number, place of birth, date of birth, and phone numbers;
- Police traffic collision report with full names, dates of birth, and addresses for three people, driver's license numbers for two of the three; and
- A contractor's full name, partial social security number, signature, and date of birth.

General Proprietary Business Information. General proprietary business information is information related to a company's products, business operations, or activities. This information could reveal a company's trade secrets or business practices and be exploited by competitors. Examples include financial information, trade secrets, product research and development, existing and future product designs, and company performance details.

Of the 116 exposed CUI documents we found during our limited testing, 23 (19.8 percent) have general proprietary business CUI. Specific examples include the following:

- Twelve proprietary customer satisfaction surveys the vendor labeled as containing proprietary research, copyrighted materials, and literary property of [REDACTED]. The surveys include a notice that they need to be "safeguarded, allowing no one to duplicate or change the contents in an effort to formulate an inferior product."
- Ten vendor responses to GSA requests for quotations, which contain technical and pricing information, such as labor rates. One document has the following marking: "THIS PROPOSAL INCLUDES DATA THAT SHALL NOT BE DISCLOSED OUTSIDE THE GOVERNMENT AND SHALL NOT BE DUPLICATED, USED, OR DISCLOSED—IN WHOLE OR IN PART—FOR ANY PURPOSE OTHER THAN TO EVALUATE THIS PROPOSAL." (emphasis in the original)
- A review document for the design of the [REDACTED]. This document has the following marking: "C U I CONFIDENTIALITY NOTICE: This Google Drive Document and any supporting documents, including supplemental email attachments are for the exclusive and confidential use of the intended recipient and may contain information that is privileged, confidential, proprietary, and exempt from disclosure." (emphasis in the original)

Exposures of general proprietary business information can have adverse consequences for affected companies. For example, exposure of proprietary information, such as company trade secrets or information on product research and development, can result in significant loss of market share and corresponding financial losses.

Although we reviewed a relatively small number of documents, the volume of CUI found during our limited search indicates that more CUI may be exposed in GSA's Google Drive. GSA must ensure that this information is properly secured to protect against potential misuse, including physical security risks and financial harm.

GSA's Oversight of CUI in Its Google Drive Did Not Detect the CUI Exposures

Overall, we found that GSA did not detect the CUI exposures in its Google Drive due to deficiencies in its oversight of CUI. As detailed below, we found deficiencies in GSA's: (1) management of a third-party data loss prevention tool used to prevent and detect CUI exposures; and (2) policies, guidance, and procedures governing CUI.

GSA does not effectively manage the third-party data loss prevention tool used to prevent and detect CUI exposures in Google Drive. In August 2014, GSA implemented a third-party software application, which it uses as a data loss prevention tool, to protect against CUI exposures. However, we found the following deficiencies in GSA's management of this tool:

- GSA has not fully completed annual reviews of the data loss prevention tool's search terms to ensure effective detection of CUI;
- Searches using the data loss prevention tool did not detect exposed documents that included current search terms;
- GSA did not incorporate many relevant terms from the Agency CUI guidance into the data loss prevention tool's search terms;
- GSA did not implement an available data loss prevention tool feature that could prevent some CUI exposures;
- GSA was unaware of the data loss prevention tool's file size limitation; and
- GSA did not document program decisions affecting CUI protection in its Google Drive.

We discuss these issues in more detail below.

GSA has not fully completed annual reviews of the data loss prevention tool's search terms to ensure effective detection of CUI. GSA's standard operating procedure (SOP) for managing the data loss prevention tool requires the Office of GSA IT's Security Operations Division to review the tool's search terms at least annually. The SOP states that searches "need to be kept current with the terms and phrases which are sensitive to GSA" to be effective in detecting sensitive information. The annual review consists of reviewing the effectiveness of current search terms, working with Agency staff to identify new search terms, and getting proposed changes approved and implemented.

However, GSA's Security Operations Division did not fully comply with the SOP requirement to conduct the annual review. GSA IT staff initially told us that they rarely assess or adjust the data loss prevention tool's search terms. When asked when the staff last completed an annual review, the Division Director said it was difficult to know because the GSA personnel responsible for those reviews are no longer with the Agency.

In response to our request for all available annual review results from 2015 through 2024, GSA provided a spreadsheet that contained the status of the annual reviews. However, the document was incomplete. As shown in *Figure 4* on the next page, the document was missing

results for 5 years. The document was also incomplete because it did not show how GSA's Security Operations Division completed the review process for the other years provided. For example, the information for 2024 does not show how the Security Operations Division reviewed the effectiveness of current search terms, worked with GSA staff to identify new search terms, or approved and implemented proposed changes.

Figure 4. Audit Team's Assessment of GSA's Annual Review of the Data Loss Prevention Tool Search Terms

Year	Completion Status of Annual Reviews
2015	Annual review information was missing for this year.
2016	Document provided does not show that GSA fully completed the review process.
2017	Document provided does not show that GSA fully completed the review process.
2018	Annual review information was missing for this year.
2019	Document provided does not show that GSA fully completed the review process.
2020	Document provided does not show that GSA fully completed the review process.
2021	Annual review information was missing for this year.
2022	Annual review information was missing for this year.
2023	Annual review information was missing for this year.
2024	Document provided does not show that GSA fully completed the review process.

A GSA IT Specialist told us that the missing annual review documents were due to personnel changes within GSA's Security Operations Division.

Searches using the data loss prevention tool did not detect exposed documents that included current search terms. The data loss prevention tool searches the content of documents shared GSA-wide in GSA's Google Drive for certain words or phrases related to CUI. However, the tool did not detect current search terms in sensitive document labels for 40 of the 116 exposed CUI documents (34.5 percent) identified during our audit. In some cases, the documents included multiple search terms that the tool did not detect.⁹

For example, we found that the data loss prevention tool did not detect the following current search terms:

- **Controlled Unclassified Information** – Although “Controlled Unclassified Information” is a current search term, we found four exposed CUI documents that included this term. The exposed documents included information systems vulnerability information.
- **For Official Use Only** – Although “For Official Use Only” is a current search term, we found 34 exposed CUI documents that included this term. The exposed documents included information systems vulnerability information and physical security information, among other types of CUI.

⁹ Since some of the CUI documents found included more than one search term, the total number in the examples exceeds 40 instances of search terms the tool did not detect.

- **Sensitive But Unclassified** – Although “Sensitive But Unclassified” is a current search term, we found five exposed CUI documents that included this term. The exposed documents included building security information.

The Director of GSA’s Security Operations Division asserted that the data loss prevention tool may not have detected the exposed documents due to a weakness that prevented the tool from operating as intended. However, we were not able to determine specifically why the data loss prevention tool did not detect the exposed documents described above.

GSA did not incorporate many relevant terms from the Agency CUI guidance into the data loss prevention tool’s search terms. GSA’s data loss prevention tool searches do not incorporate many of the terms listed in the following GSA CUI guidance:

- **Controlled Unclassified Information (CUI) GSA Marking Manual** – This manual states that CUI should be marked with the term “CUI” and that other agencies may use the term “CONTROLLED.” However, GSA’s data loss prevention tool searches do not include either of these terms.
- **GSA’s CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use** – In this document, we identified 136 terms that are specific to GSA and could be used in the tool’s search terms. Although GSA included 10 of these terms in the tool’s searches, it did not include the remaining 126 terms. Examples of the excluded terms include the following:
 - Personally identifiable information,
 - Occupant emergency plan,
 - Business continuity of operations plan,
 - Detention cell, and
 - Driver’s license number.

GSA staff said they did not know whether GSA considered these documents when designing or reviewing the tool’s search terms.

GSA did not implement an available data loss prevention tool feature that could prevent some CUI exposures. The data loss prevention tool includes an optical character recognition (OCR) feature. This feature enhances data loss prevention by scanning images for search terms. The commercial vendor publicly announced the release of OCR and other new features on its website in June 2023 and notified GSA of the availability of the OCR feature in October 2023.

However, GSA’s Security Operations Division did not implement the OCR feature, limiting the tool’s ability to detect exposed CUI. For example, the OCR feature could have prevented some of the data exposures mentioned in our April 2025 alert memorandum.¹⁰ Specifically, the OCR

¹⁰ Memorandum Number A250043-2.

feature could have read a CUI image embedded in a safety survey for the [REDACTED] that showed detailed blueprints of the former [REDACTED].

The Security Operations Division Lead told us the division was not aware of the OCR feature until we issued our alert memorandum in April 2025 because it does not assess new releases of the data loss prevention tool. The Security Operations Division Director subsequently told us that the Security Operations Division was reviewing the feature but had not yet implemented it due to other priorities.

GSA was unaware of the data loss prevention tool's file size limitation. In response to our April 2025 alert memorandum, the former Acting GSA Administrator, Stephen Ehikian, wrote that the data loss prevention tool did not flag 10 of the 15 documents exposed in GSA's Google Drive because the tool cannot scan documents larger than 15 megabytes (MB). However, the Security Operations Division Director and Division Lead said they were not aware of this limitation until we issued our alert memorandum in April 2025.

Of the 116 CUI documents we found exposed to all GSA's Google Drive users, 14 (12.1 percent) were larger than 15 MB. These documents included a progressive collapse analysis report for the [REDACTED]; and floor plans showing sensitive areas for the [REDACTED].

The CUI detection problems arising from the data loss prevention tool's 15 MB limitation are compounded by GSA's limited insight into documents stored in its Google Drive. For example, GSA's Google Workspace administrators told us that Google Drive cannot track and inventory files larger than 15 MB, and Google's reporting tools do not offer the ability to search by file size.

GSA did not document program decisions affecting CUI protection in its Google Drive. GSA's Security Operations Division did not document program decisions affecting CUI protection in its Google Drive. As a result, Security Operations Division staff could not explain why the division discontinued some data loss prevention tool search terms, as well as other program decisions affecting CUI protection in GSA's Google Drive. For example, the Security Operations Division deactivated nine data loss prevention tool search terms that monitor Google Drive for documents shared outside GSA. These search terms were designed to detect personally identifiable, legal, and physical security information. However, the Security Operations Division did not document its reason for deactivating these search terms.

GSA IT staff could not explain why the search terms were deactivated. They stated that the personnel involved are no longer employed by GSA, and they did not document the rationale for their decisions. They added that GSA plans to consider reactivating these search terms for potential use.

Deficiencies in GSA's Policies, Guidance, and Procedures Governing CUI in Google Drive

We also found the deficiencies in GSA's policies, guidance, and procedures related to protecting CUI described below:

- **Lack of a Sharing Approval Process** – GSA policies allow all users of its Google Drive to share a document with all of GSA without prior approval. The *GSA Controlled Unclassified Information (CUI) Program Guide* instructs employees to limit access of CUI stored in GSA's Google Drive to those with a lawful government purpose. However, GSA's Information System Security Manager for Google Workspace said nothing prevents employees from granting unlimited access to CUI. They said staff can create a shared drive, add terabytes of PII to it, and then share it with whomever they feel should have access. As a result, GSA staff have exposed CUI to all of GSA's Google Drive users.

When we discussed this with GSA IT officials, a Supervisory IT Specialist said they were evaluating a process to require supervisor approval to share documents with all users of GSA's Google Drive.

- **Lack of Standard Naming Conventions** – As previously noted, GSA uses and manages a commercially available data loss prevention tool to search GSA's Google Drive for CUI exposed to all GSA users. If GSA used a standard naming convention for CUI documents, this tool could more effectively identify and protect exposed CUI because naming conventions make it easier to identify and manage documents in shared environments like Google Drive.

However, GSA's *Controlled Unclassified Information (CUI) Policy* and *Controlled Unclassified Information (CUI) GSA Marking Manual* do not include standard naming conventions for all CUI documents. The manual only states that it is a best practice to include an indicator such as [Contains CUI] at the end of the document name when emailing CUI outside of the GSA network (gsa.gov).

- **The SOP for Managing the Data Loss Prevention Tool Does Not Clearly Define Roles and Responsibilities** – As noted previously, GSA's SOP for managing the data loss prevention tool requires GSA's Security Operations Division to review the tool's search terms at least annually. However, the SOP does not state which staff should perform and approve the annual review. Clearly defined roles and responsibilities would improve the consistency and quality of annual reviews and promote accountability to ensure the reviews are completed and approved. The GSA Security Operations Division Director agreed that adding this information is necessary.

In sum, GSA is not effectively protecting information stored in its Google Drive, resulting in unauthorized exposures of CUI. Accordingly, GSA should take appropriate measures to protect

CUI that is currently exposed in its Google Drive and strengthen internal controls to prevent further exposures.

Conclusion

GSA is not effectively protecting information stored within its Google Drive, resulting in unauthorized exposures of CUI. During a limited search of GSA's Google Drive, we found 116 files containing CUI that were improperly shared with all GSA users. As a result, the CUI was exposed to GSA employees and contractors who did not have a legitimate business need to know.

GSA did not detect that the CUI was exposed in its Google Drive because of deficiencies in its oversight. Specifically, we found deficiencies in GSA's: (1) management of a third-party data loss prevention tool used to prevent and detect CUI exposures; and (2) policies, guidance, and procedures governing CUI.

GSA must ensure the proper management and maintenance of CUI stored in its Google Drive. Accordingly, GSA should immediately restrict access to the 116 documents containing CUI that were identified during our audit to prevent improper access. GSA should also identify and restrict any other CUI documents that are improperly exposed to all GSA users and follow GSA's policy to identify and notify the individuals affected by the exposed information. Additionally, GSA should strengthen controls to prevent future CUI exposures in its Google Drive.

Recommendations

We recommend that the GSA Chief Information Officer:

1. Restrict access for all 116 CUI documents exposed in GSA's Google Drive to only GSA users with a lawful government purpose to access that information.
2. Identify other CUI documents exposed to all GSA users not found during this audit and restrict these documents to only GSA users with a lawful government purpose to access that information.
3. Identify and notify the individuals affected by the exposed information in accordance with the *GSA Information Breach Notification Policy*.
4. Identify and implement additional controls to ensure that Agency employees only share CUI documents in GSA's Google Drive with users who have a lawful government purpose to access that information. At a minimum:
 - a. Implement an approval process for sharing CUI documents in Google Drive with all GSA users.
 - b. Develop a standard naming convention for CUI documents to more effectively identify and protect CUI in GSA's Google Drive.
 - c. Update Agency guidance and training materials to further emphasize the importance of CUI, the different categories of CUI, and how to appropriately flag CUI documents in Google Drive.

5. Improve management of the data loss prevention tool to better detect and prevent CUI exposures in GSA's Google Drive. Specifically, GSA's Security Operations & Engineering Division should:
 - a. Review, update, enforce, and document the process for the annual review of the data loss prevention tool's search terms.
 - b. Incorporate relevant terms from GSA's CUI guidance into the data loss prevention tool's search terms.
6. Assess and implement available enhancements to the data loss prevention tool to maximize detection and restriction of CUI exposures in GSA's Google Drive. The Security Operations & Engineering Division should:
 - a. Evaluate the current data loss prevention tool's OCR feature for implementation.
 - b. Develop a process for evaluating new data loss prevention tool features for implementation.
 - c. Evaluate methods to identify exposed CUI documents larger than 15 MB and safeguard those documents.
7. Develop and implement a process to document and maintain management and operational decisions for the data loss prevention tool.

GSA Comments

GSA's Chief Information Officer agreed with our recommendations. GSA's comments are included in their entirety in **Appendix E**.

Appendix A – Objective, Scope, and Methodology

Objective

We performed this audit to assess security controls and privacy settings used to protect CUI stored in GSA's Google Drive. Our objective was to assess the effectiveness of security controls and privacy settings in place to protect the confidentiality, integrity, and availability of information stored within GSA's Google Drive as required by federal and Agency information technology security policies, procedures, standards, and guidance.

Scope and Methodology

To accomplish our objective, we:

- Reviewed laws, regulations, policies, and guidance to establish audit criteria;
- Reviewed prior GSA Office of Inspector General audit reports and memorandums to identify issues regarding the protection of sensitive information and the actions taken to limit unauthorized exposure;
- Performed keyword searches in GSA's Google Drive for documents shared with all users to determine if they contain CUI;
- Assessed GSA's management and oversight of its use of Google Drive;
- Analyzed GSA policies and guidance related to its use of the data loss prevention tool to detect and prevent CUI exposures in GSA's Google Drive;
- Assessed the design, implementation, and operating effectiveness of relevant internal controls; and
- Interviewed and corresponded with GSA officials and staff involved in the management and oversight of GSA's Google Drive and its data loss prevention tool.

Sampling

We used judgmental sampling to determine whether GSA exposed CUI documents in its Google Drive, which contains 2.5 million documents. We searched GSA's Google Drive using 39 keywords drawn from GSA's *CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use* and the *GSA Controlled Unclassified Information (CUI) Program Guide*.

We limited our search to documents shared with all GSA Google Drive users. For each keyword, we reviewed search results until we identified 10 or more exposed CUI documents. We identified 116 documents that contained exposed CUI. Because we used a judgmental sample, we cannot project these results to the full population. However, the sample was sufficient to address our audit objective.

Internal Controls

We assessed internal controls significant within the context of our audit objective against internal control guidance for federal agencies. The methodology above describes the scope of our assessment, and the report finding includes any internal control deficiencies we identified. Our assessment is not intended to provide assurance on GSA's internal control structure as a whole. GSA management is responsible for establishing and maintaining internal controls.

Compliance Statement

We conducted the audit between March and December 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Appendix B – CUI Categories

This table includes the CUI categories we tested to determine if GSA properly restricted access to CUI in its Google Drive. The CUI category names and descriptions are from the GSA’s *CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use* document. Our test included 9 of GSA’s 23 CUI categories based on our ability to search for relevant keywords related to the categories.

CUI Category	Description
Collective Bargaining	Information concerning agencies’ and representatives’ duty to negotiate in good faith, to include disclosure of certain labor relations training and guidance materials and limiting the issuance of certain subpoenas.
Emergency Management	Information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.
Entity Registration Information	Non-public information collected during entity registration in the System for Award Management, the common source of vendor data for the U.S. government.
General Privacy	Personal information, or, in some cases, “personally identifiable information,” as defined in Office of Management and Budget M-17-12; or “means of identification” as defined in 18 U.S.C. 1028(d)(7).
General Procurement and Acquisition	The acquisition and procurement of goods and services, including, but not limited to, cost or pricing data, contract information, indirect costs, and direct labor rates.
General Proprietary Business Information	Company products, business, or activities, including, but not limited to, financial information, data, or statements; trade secrets; product research and development; and existing and future product designs and performance specifications.
Information Systems Vulnerability Information	Information that if not protected, could result in adverse effects to information systems.
Physical Security	Protection of federal buildings, grounds, or property.
Source Selection	According to Federal Acquisition Regulation (FAR) 2.101, <i>Definitions</i>, source selection information is any information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly. Examples listed in the FAR include: • Bid prices submitted in response to an agency invitation for bids; • Proposed costs or prices submitted in response to an agency solicitation; • Source selection plans; • Technical evaluation plans; and • Technical evaluations of proposals.

Appendix C – List of 39 Terms Used to Search GSA’s Google Drive for Exposed CUI

This table includes search terms taken from or related to GSA’s *CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use* document and the *GSA Controlled Unclassified Information (CUI) Program Guide* that we used in our limited testing for CUI exposed to all users of GSA’s Google Drive.

#	Search Term	CUI Category/Marking
1	Bank account number	General Privacy
2	[REDACTED]	Physical Security
3	[REDACTED]	Physical Security
4	[REDACTED]	Physical Security
5	[REDACTED]	Physical Security
6	[REDACTED]	Physical Security
7	Collective bargaining	Collective Bargaining
8	Controlled unclassified information	Marking
9	CUI	Marking
10	[REDACTED]	Physical Security
11	[REDACTED]	Physical Security
12	For official use only	Legacy Marking
13	FOUO	Legacy Marking
14	[REDACTED]	Physical Security
15	IT contingency plan	Information Systems Vulnerability Information
16	ITCP	Information Systems Vulnerability Information
17	Legal and discovery	Collective Bargaining
18	Network diagram	Physical Security
19	[REDACTED]	Emergency Management
20	[REDACTED]	Emergency Management
21	Plan of action and milestones	Information Systems Vulnerability Information
22	POA&M	Information Systems Vulnerability Information
23	[REDACTED]	Physical Security
24	[REDACTED]	Physical Security
25	[REDACTED]	Information Systems Vulnerability Information
26	SBU	Legacy Marking
27	[REDACTED]	Physical Security
28	[REDACTED]	Physical Security
29	[REDACTED]	Information Systems Vulnerability Information
30	Sensitive but unclassified	Legacy Marking
31	[REDACTED]	Physical Security
32	Social security number	General Privacy

#	Search Term	CUI Category/Marking
33	Source selection	Source Selection
34	SSN	General Privacy
35	SSP	Information Systems Vulnerability Information
36	SSPP	Information Systems Vulnerability Information
37	System security and privacy plan	Information Systems Vulnerability Information
38	System security plan	Information Systems Vulnerability Information
39	This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal.	General Procurement and Acquisition

Appendix D – List of 116 CUI Documents Exposed in GSA’s Google Drive to All Users¹¹

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
1.	[REDACTED] [REDACTED] [REDACTED]	Physical Security – Site plans for the [REDACTED], with building security information like badge holder and visitor routes, screening techniques, entrances, pre-screen areas and technology, magnetometers, x-rays, and interview rooms.
2.	[REDACTED]	Emergency Management – Continuity of Operations Plan (COOP) for [REDACTED] is intended for a “need-to-know basis” so as not to “endanger the lives and privacy of employees” and “compromise the security of essential equipment, services, and systems of [REDACTED].”
3.	[REDACTED] [REDACTED]	Physical Security – Progressive collapse analysis for the [REDACTED], which includes building security information. It describes the building’s collapse vulnerabilities, critical failure locations, and includes diagrams.
4.	[REDACTED] [REDACTED]	Physical Security – Operational requirements for the [REDACTED]’s Top Secret/Special Compartmented Information IT and communications networks. It includes a floor plan of sensitive areas.
5.	[REDACTED]	Emergency Management – COOP for the [REDACTED] outlines planning scenarios, including events affecting other buildings and the entire [REDACTED].
6.	[REDACTED]	Physical Security – Material Fielding Agreement describes the Top Secret-Sensitive Compartmented Information virtual enterprise system for the [REDACTED]. It includes a parts list and floor plan.
7.	[REDACTED]	Emergency Management – Occupant Emergency Plan for the [REDACTED] and [REDACTED] at the [REDACTED]. It identifies the floors the [REDACTED] and [REDACTED] occupy, designated assembly points during an evacuation, with a map and a list of assembly groups.
8.	[REDACTED]	Physical Security – Drawings for the [REDACTED], showing sensitive criminal investigation space, seized evidence room, cross-section of the building, and partial roof plan.
9.	[REDACTED] [REDACTED]	Physical Security – Construction and design project document includes site plans and floor plans showing sensitive interview and hold room for the [REDACTED].
10.	[REDACTED] [REDACTED] [REDACTED]	Physical Security – Updated feasibility study for the [REDACTED], which includes floor plans showing sensitive areas for juries, public defenders, witnesses, U.S. attorneys, and judges’ chambers.
11.	[REDACTED] [REDACTED] [REDACTED]	Physical Security – Feasibility study for the [REDACTED], has floor plans showing sensitive areas for juries, public defenders, witnesses, U.S. attorneys, and judges’ chambers.
12.	[REDACTED] [REDACTED] [REDACTED]	Information Systems Vulnerability Information – Concept of Operations for the Continuous Monitoring as a Service solution provided by the [REDACTED]. It covers Hardware Asset Management, Software Asset Management, Configuration Setting Management, Vulnerability Management, and aspects of identity and access management.

¹¹ Document titles are taken verbatim from the source documents.

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
13.	[REDACTED]	Physical Security – These floor plans show sensitive areas, such as the location for the judges’ chamber at the [REDACTED].
14.	[REDACTED]	General Proprietary Business Information – Customer Satisfaction Surveys. They contain proprietary research, copyrighted materials, and literary property of [REDACTED].
15.	[REDACTED]	
16.	[REDACTED]	
17.	[REDACTED]	
18.	[REDACTED]	
19.	[REDACTED]	
20.	[REDACTED]	
21.	[REDACTED]	
22.	[REDACTED]	
23.	[REDACTED]	
24.	[REDACTED]	
25.	[REDACTED]	
26.	[REDACTED]	Physical Security – Statement of work contains building security information for the [REDACTED]. It outlines security guard egress requirements for an unsecured probation door during jury trials.
27.	[REDACTED]	Physical Security – Laminated security glazing and bullet-resistant glazing requirements for a [REDACTED].
28.	[REDACTED]	Physical Security – Security screening and a perimeter security barrier information for the [REDACTED]. The structural designs include blast, progressive collapse, and seismic mitigation measures. The floor plans show sensitive water and electrical rooms, childcare center, and the [REDACTED].
29.	[REDACTED]	Physical Security – Feasibility study for the [REDACTED], includes the building security level and building automation system. It also describes the security equipment used at the front lobby security checkpoint and the building’s fire protection and life safety system.
30.	[REDACTED]	Physical Security – Statement of work for creating a new break/training room at the [REDACTED]. It describes building security information, which GSA lists as CUI.
31.	[REDACTED]	Physical Security – This presentation of the Department of Defense’s support for the 2013 [REDACTED] includes physical security CUI for the protection of the executive and congressional branch officials and buildings.
32.	[REDACTED]	Emergency Management – This Occupant Emergency Plan for the [REDACTED], outlines procedures to protect personnel and property during emergencies.
33.	[REDACTED]	General Privacy – Contains a contractor’s PII, including name, last four digits of the social security number, signature, and date of birth.
34.	[REDACTED]	Information Systems Vulnerability Information – A draft System Security Plan for the [REDACTED].
35.	[REDACTED]	Information Systems Vulnerability Information – A draft System Security Plan for the [REDACTED].
36.	[REDACTED]	Physical Security – This is a technical diagram of the information technology (IT) network for the [REDACTED].

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
37.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
38.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
39.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
40.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
41.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
42.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
43.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
44.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
45.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
46.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
47.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
48.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
49.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
50.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
51.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
52.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
53.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
54.	[REDACTED]	Physical Security – This is a technical diagram of the IT network for the [REDACTED].
55.	[REDACTED]	Physical Security – Preliminary design concepts for the U.S. courthouse in the [REDACTED], which includes floor plans showing sensitive security screening areas, sally ports, the U.S. attorney's office, holding cells, courtrooms, jury suites, and judges' chambers. [REDACTED].
56.	[REDACTED]	Physical Security – Document includes floor plans for the [REDACTED], that show sensitive gun lockers, judge's chambers, jury rooms, metal detectors, and x-ray screening areas.
57.	[REDACTED]	Physical Security – Blast vulnerability assessment for the [REDACTED]. The assessment analyzed damage caused by explosive devices, including man-portable external, suicide/homicide bomber, and vehicle borne.

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
58.	[REDACTED]	Physical Security – Contains diagrams and floorplans for the [REDACTED], including sensitive judges' parking spaces, sally port, and judges' and prisoners' restricted circulation areas.
59.	[REDACTED] [REDACTED]	Physical Security – Feasibility study for the [REDACTED], describes building security level, automation system, security equipment used at the security checkpoint in the front lobby, and the building's fire protection and life safety system.
60.	[REDACTED]	General Privacy – Declaration of federal employment form contains an applicant's PII, including full name, social security number, place of birth, date of birth, and phone numbers.
61.	[REDACTED] [REDACTED]	General Privacy – Motor vehicle accident report contains PII for two people, including full names, addresses, and telephone numbers for both; driver's license number and date of birth for one.
62.	[REDACTED] [REDACTED]	General Privacy – Kentucky Uniform Police Traffic Collision Report contains PII for three people, including full names and dates of birth for all three, and driver's license numbers for two.
63.	[REDACTED] [REDACTED]	General Privacy – Motor vehicle accident report contains PII for three people, including full names and addresses for all three, driver's license numbers for two, and date of birth for one.
64.	[REDACTED] [REDACTED] [REDACTED] [REDACTED]	General Proprietary Business Information – Request for Quotation (RFQ) response from a vendor. The RFQ contains proprietary company information.
65.	[REDACTED] [REDACTED] [REDACTED]	General Proprietary Business Information – Request for Proposal response from a vendor containing proprietary company information.
66.	[REDACTED] [REDACTED]	General Proprietary Business Information – RFQ responses from vendors for executive coaching, facilitation, and training services.
67.	[REDACTED]	
68.	[REDACTED] [REDACTED]	
69.	[REDACTED] [REDACTED]	
70.	[REDACTED] [REDACTED]	
71.	[REDACTED] [REDACTED]	
72.	[REDACTED] [REDACTED]	
73.	[REDACTED] [REDACTED]	
74.	[REDACTED] [REDACTED]	Source Selection – Source selection information for lead design firms for the [REDACTED]. GSA considers "Assistance to customers in determining the acquisition strategy" as CUI.
75.	[REDACTED] [REDACTED] [REDACTED]	
76.	[REDACTED] [REDACTED]	Source Selection – Source selection information. GSA considers "Assistance to customers in determining the acquisition strategy" as CUI.

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
77.	[REDACTED]	Source Selection – Small business analysis contract file records include source selection information. These forms record that small business was considered. GSA considers “contract documentation for selection” as CUI.
78.	[REDACTED]	
79.	[REDACTED]	
80.	[REDACTED]	
81.	[REDACTED] ¹²	
82.	[REDACTED]	Source Selection – Acquisition plan contains source selection information. It also has “SOURCE SELECTION INFORMATION – SEE FAR PART 3.104” in the footer of every page. GSA states that FAR 3.104-4, <i>Disclosure, protection, and marking of contractor bid or proposal information and source selection information</i> , is an applicable CUI authority in GSA’s <i>CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use</i> .
83.	[REDACTED]	Source Selection – Evaluation report includes source selection information. This evaluation report investigates the financial capability of two firms. It also has the following marking: “PROPRIETARY AND/OR SOURCE SELECTION INFORMATION SEE FAR 3.104.” GSA states that FAR 3.104-4 is an applicable CUI authority in GSA’s <i>CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use</i> .
84.	[REDACTED]	Physical Security – Contains building security information that discloses the location of the existing security fence at the [REDACTED]. It also includes the location of the proposed security swing gate and relocated security fencing.
85.	[REDACTED]	Physical Security – Contains the location of the building automation system (BAS), including the location of the BAS equipment, IP address of the server, and images of the recommended Java Application Control Engine installation location for the [REDACTED].
86.	[REDACTED]	Physical Security – Contains equipment location of the BAS at three [REDACTED].
87.	[REDACTED]	Physical Security – Contains instructions on how to access the [REDACTED], including the username and password to access the servers.

¹² Since we found two different copies of [REDACTED] exposed, we counted this twice in our finding.

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
88.	[REDACTED]	Physical Security – Contains images of the BAS switch for the [REDACTED].
89.	[REDACTED]	
90.	[REDACTED]	
91.	[REDACTED]	
92.	[REDACTED]	
93.	[REDACTED]	
94.	[REDACTED]	
95.	[REDACTED]	
96.	[REDACTED]	
97.	[REDACTED]	
98.	[REDACTED]	
99.	[REDACTED]	
100.	[REDACTED]	
101.	[REDACTED]	Physical Security – Contains detailed structural descriptions of the [REDACTED], such as blast resistance design and images of the building’s framing floor plan. It also includes the building’s facility security level and counterterrorism methods taken to protect building occupants.
102.	[REDACTED]	
103.	[REDACTED]	Physical Security – Contains the facility security level for [REDACTED]. It also includes counterterrorism methods taken to protect building occupants. This includes security perimeter cameras, vehicle intrusion barriers, progressive collapse resistance, intrusion detection, and location of blast resistant areas.
104.	[REDACTED]	Physical Security – Contains counterterrorism methods taken to protect building occupants. This includes detailed structural descriptions of the [REDACTED], and the building’s facility security level. It also includes the previous window vulnerability assessment noting that the existing windows do not meet the blast load performance criteria, and that retrofits will be required to meet the blast load performance requirements.
105.	[REDACTED]	Physical Security – Contains building operation plans with details in the event of a disaster recovery for [REDACTED]. It also explains what happens if a disaster recovery situation occurs. Details include the number of building generators, amount of fuel needed to run the generator, and generator run capacity.
106.	[REDACTED]	General Procurement and Acquisition – Contains the marking of “CUI” on all pages. The document includes a process map, substantial supply chain risk, roles and responsibilities, steps of process map, and a reporting template.
107.	[REDACTED]	General Proprietary Business Information – Contains the marking “CUI” on all six worksheets. The spreadsheets are the comment log for the design of the [REDACTED].

#	Document Title	CUI Category and Description of Sensitive Information in Each Document
108.	[REDACTED]	Physical Security – Contains the marking “CUI” on each worksheet. The document contains the technical interpretation of design and regulatory standards for architecture, engineering, historic preservation, interior design, sustainability, environmental impact analysis, and urban planning, which the document considers “CUI” and should not be shared domain-wide.
109.	[REDACTED]	
110.	[REDACTED]	
111.	[REDACTED]	Information Systems Vulnerability Information – Contains the marking “Controlled Unclassified Information.” This document describes service specifications for Activity Address Code Assignment web service specifications. It contains interaction protocol, policies and quality of service requirements, name of the service provider, detailed service design, the three main operations of web service methods, and web service definition.
112.	[REDACTED]	Information Systems Vulnerability Information – Contains the marking “Controlled Unclassified Information.” This document contains master data information, like specific files transferred through the Master Data Interface, assumptions, system identification, interface description, description of data, system touch points, file naming convention, file structure, and security requirements.
113.	[REDACTED]	Information Systems Vulnerability Information – Contains the marking “Controlled Unclassified Information.” This document contains a multi-faceted approach for classifying GSA content. It includes the purpose of the categorization, access control levels, folder structure, document object model, recommendation, and implementation approach.
114.	[REDACTED]	Information Systems Vulnerability Information – Contains the marking “Controlled Unclassified Information.” This study contains the file system architecture and configuration of its existing implementation.
115.	[REDACTED]	Emergency Management – Occupant Emergency Plan with the marking “Law Enforcement Sensitive – Do not disseminate – destroy by shredding.” This document details facility characteristics, protection systems, occupation information, and notification and evacuation procedures for [REDACTED].
116.	[REDACTED]	Information Systems Vulnerability Information – This Plan of Action and Milestones details the weaknesses and milestone changes of the [REDACTED].

Appendix E – GSA Comments

DocuSign Envelope ID: 185E7363-578D-844F-8338-B13FDCD9B657



**U.S. General Services
Administration**

October 5, 2026

MEMORANDUM FOR Sonya Panzo
Associate Deputy Assistant Inspector General for Auditing
Information Technology and Finance Audit Office (JA-T)

FROM: David Shive
Chief Information Officer
Office of GSA IT (I)

SUBJECT: Response to the Office of Inspector General (OIG) Draft
Report, *Controlled Unclassified Information in GSA's
Google Drive Was Improperly Exposed* (A250043)

DocuSigned by:
David Shive
A3AE4284A2754F9

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the subject draft report, in which OIG made the following recommendations:

- (1) Restrict access for all 116 CUI documents exposed in GSA's Google Drive to only GSA users with a lawful government purpose to access that information.
- (2) Identify other CUI documents exposed to all GSA users not found during this audit and restrict these documents to only those users with a lawful government purpose to access that information.
- (3) Identify and notify the individuals affected by the exposed information in accordance with the *GSA Information Breach Notification Policy*.
- (4) Identify and implement additional controls to ensure that Agency employees only share CUI documents in GSA's Google Drive with users who have a lawful government purpose to access that information. At a minimum:
 - a. Implement an approval process for sharing CUI documents in Google Drive with all GSA users.
 - b. Develop a standard naming convention for CUI documents to more effectively identify and protect CUI in GSA's Google Drive.
 - c. Update Agency guidance and training materials to further emphasize the

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

importance of CUI, the different categories of CUI, and how to appropriately flag CUI documents in Google Drive.

(5) Improve management of the data loss prevention tool to better detect and prevent CUI exposures in GSA's Google Drive. Specifically, GSA's Security Operations & Engineering Division should:

- a. Review, update, enforce, and document the process for the annual review of the data loss prevention tool's search terms.
- b. Incorporate relevant terms from GSA's CUI policies and guidance into the data loss prevention tool's search terms.

(6) Assess and implement available enhancements to the data loss prevention tool to maximize detection and restriction of CUI exposures in GSA's Google Drive. The Security Operations & Engineering Division should:

- a. Evaluate the current data loss prevention tool's optical character recognition feature for implementation.
- b. Develop a process for evaluating new data loss prevention tool features for implementation.
- c. Evaluate methods to identify exposed CUI documents larger than 15 megabytes and safeguard those documents.

(7) Develop and implement a process to document and maintain management and operational decisions for the data loss prevention tool.

GSA IT concurs with the recommendations and is working on a plan to address them. Please note that GSA IT's review determined that the identified documents were not exposed externally, and that, based on file access reviews and user interviews, there was no indication of malicious intent.

While this audit was underway, GSA IT took significant corrective actions to strengthen the protection of sensitive information across GSA's Google Workspace. GSA IT implemented enterprise-wide actions to reduce the risk of improper CUI exposure including: 1) updating existing internal procedures and security workflows, and notified employees of their responsibilities for secure information sharing, 2) reviewing documents shared domain-wide and restricting access as appropriate, 3) evaluating additional controls and tools to flag CUI exposures, 4) revisiting training and communications on secure sharing practices, and 5) completing necessary policy and process updates. Following testing and evaluation, GSA IT has also deployed Optical Character Recognition within the CloudLock environment to improve detection of sensitive markings embedded in images.

If you have any questions, please contact Mindy Levit, Director, IT Audit and Records Management at mindy.levit@gsa.gov.

Appendix F – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Chief Information Officer (I)

GSA IT Chief of Staff (I)

Associate Chief Information Officer (IA)

Chief Information Security Officer (IS)

Acting PBS Commissioner (P)

PBS Deputy Commissioner (P1)

PBS Chief of Staff (P1A)

Acting Federal Acquisition Service Commissioner (F)

Acting Federal Acquisition Service Deputy Commissioner (F1)

Federal Acquisition Service Chief of Staff (F1A)

Chief Financial Officer (B)

Deputy Chief Financial Officer (B)

Audit Management Division (BPA)

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](https://www.linkedin.com/company/gsa-oig)



[gsa_oig](https://twitter.com/gsa_oig)



[@gsa-oig](https://www.facebook.com/gsa-oig)



[gsa-oig](https://www.instagram.com/gsa-oig)
