



Office of Forensic Auditing, Evaluation and Analysis
Office of Inspector General
U.S. General Services Administration

INSPECTION REPORT

Security Vulnerabilities – Protecting Information and Property in the GSA Central Office Open Space

Report Number: JE15-001
October 16, 2014

REPORT ABSTRACT

OBJECTIVE

Our objective was to identify weaknesses in the physical security of sensitive information and highly pilferable government-furnished personal property in the open office space at the GSA Central Office.

*Office of Forensic
Auditing, Evaluation and
Analysis (JE)
1800 F Street, NW,
Suite 5013
Washington, DC 20405
202-273-4989*

Security Vulnerabilities – Protecting Information and Property in the GSA Central Office Open Space

Report Number: JE15-001

October 16, 2014

What We Found

We identified the following during our inspection:

1. Physical control weaknesses in securing sensitive information covered by the Privacy Act (5 U.S.C. § 552a) and the Trade Secrets Act (18 U.S.C. § 1905).
2. Physical control weaknesses in securing highly pilferable government-furnished personal property.

What We Recommend

Based on our findings we recommend GSA supervisors and managers:

1. Enforce GSA policies and procedures for the safeguarding of Personally Identifiable Information, other sensitive information, and highly pilferable government-furnished personal property.
2. Routinely monitor for security compliance by both employees and contractors.
3. Assess the adequacy of secure storage space available to meet employee and contractor needs.

Management Comments

The Chief of Staff concurred with our recommendations and launched a campaign educating employees of the associated policies and procedures. Management's comments can be found in their entirety in **Appendix B**.



U.S. General Services Administration
Office of Inspector General

DATE: October 16, 2014

TO: ADAM NEUFELD
Chief of Staff (AC)

Patricia D. Sheehan

FROM: PATRICIA D. SHEEHAN
Director
Office of Forensic Auditing, Evaluation and Analysis (JE)

SUBJECT: Inspection Report
Security Vulnerabilities – Protecting Information and Property in the GSA
Central Office Open Space
Report Number: JE15-001

This report presents the results of our inspection of the GSA Central Office conducted on July 30, 2014. Our findings and recommendations are summarized in the Report Abstract. Instructions regarding the resolution process can be found in the email that transmitted this report.

Your written comments to the draft report are included in **Appendix B** of this report.

If you have any questions regarding this report, please contact me or any member of the Inspection team at the following:

Patricia Sheehan	Director	Patricia.Sheehan@gsaig.gov	202-273-4989
Natalie Granito	Auditor	Natalie.Granito@gsaig.gov	202-273-7267
Rashawna Chapman	Management Analyst	Rashawna.Chapman@gsaig.gov	202-273-7252
Gabrielle Perret	Management Analyst	Gabrielle.Perret@gsaig.gov	202-273-7268

On behalf of the inspection team, I would like to thank you and your staff for your assistance during this inspection.

RESULTS IN BRIEF

On July 30, 2014, the OIG Office of Forensic Auditing, Evaluation and Analysis conducted an after-hours limited inspection of the open office space at the General Services Administration (GSA) Central Office. The inspection identified physical control weaknesses in securing sensitive information covered by the Privacy Act (5 U.S.C. § 552a) and the Trade Secrets Act (18 U.S.C. § 1905), as well as physical control weaknesses in securing highly pilferable government-furnished personal property.

The inspection of the GSA Central Office open space found numerous incidences of unsecured Personally Identifiable Information (PII)¹ and other sensitive information.² The inspection found an unsecured HSPD-12 PIV card, sensitive contract files, architectural drawings marked “SENSITIVE BUT UNCLASSIFIED,” unlocked file cabinets containing sensitive information, a combination code for a bay of personal lockers that was left directly on top of those lockers, and a door cipher lock combination taped to the back of the door. The inspection also found valuable property that was unsecured, including laptops and other electronics.

This report discusses the results of the OIG’s inspection of the GSA Central Office, and recommends that GSA managers and supervisors: (1) enforce GSA policies and procedures for the safeguarding of PII, other sensitive information, and highly pilferable government-furnished personal property; (2) routinely monitor for security compliance by both employees and contractors; and (3) assess the adequacy of secure storage space available to meet employee and contractor needs.

BACKGROUND

The GSA Central Office renovation Phase I, completed for employee reoccupation in 2013, created an open space work environment that eliminated traditional office doors and cubicles in favor of a desk and conference room reservation system with few permanent desk assignments. GSA’s traditional office space was previously secured by office suites with locked doors. The open workspace has created a new environment in which employees now have open-concept offices with “hotel desks”³ that feature personal lockers and locking file cabinets. The transition to a more collaborative workspace has increased security risks for vulnerable assets and sensitive

¹ Personally Identifiable Information (PII), as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.

² For the purposes of this report, “sensitive information” is any information GSA has determined requires some degree of heightened protection from unauthorized access, use, disclosure, disruption, modification, or destruction because of the nature of the information, e.g., personal information required to be protected by the Privacy Act of 1974, proprietary commercial information, information critical to agency program activities, and information that has been or may be determined to be exempt from public release under the Freedom of Information Act.

³ For this report we define hotel desks in accordance with GSA’s Successful Hoteling: GSA’s 10 Tips as “Hoteling is the office management strategy that considers certain office resources, such as workspaces and equipment, to be shared assets, rather than assets ‘owned’ by specific individuals within an organization....Hoteling is typically characterized by reservation and check-in processes.” http://www.gsa.gov/graphics/admin/Successful-Hoteling-Tips_Final.pdf, retrieved September 8, 2014.

information as GSA employees adjust to taking new steps to physically secure property and information in their personal workspaces.

In addition to the many GSA directives that broadly address controls to protect property and sensitive information,⁴ GSA has also communicated specific guidance to address the new open office space through a blog series of frequently asked questions targeting issues employees may experience during the transition.⁵ These blog entries discussed a variety of security issues in the new open office environment, including:

Employees working on sensitive material or information will have to be diligent about monitoring their environment and securing information as necessary. Materials can be secured in shared filing cabinets, in employee personal storage, or for a short period, in the locking peds⁶ that are at the workstation.

Furthermore, GSA's intranet site contains a training presentation entitled, "GSA Central Office, Office of Theft Prevention Training, June 2014, Crime Prevention Tips," with suggestions for reducing the potential for theft in the workplace. The training emphasizes precautions all employees and contractors could take to prevent burglary, theft, or vandalism, such as:

- Lock all offices, conference rooms, or storage rooms that are regularly unoccupied.
- If you are the last to leave at night, secure all computer systems, critical files, and copiers.
- When employees must work before or after business hours they should keep their doors locked.

Moreover, GSA employees and contractors are required to take annual training, "IT Security Awareness and Privacy 101 Training," that highlights requirements for protecting PII. Finally, when using GSA's collaborative work system, users are required to acknowledge their responsibility to safeguard GSA property and information by agreeing to:

- Protect and conserve Government resources and assets from theft, destruction and use for other than authorized purposes.
- Physically secure highly pilferable and/or sensitive items that are in their custody when their office spaces or buildings are unoccupied.
- Employ locking devices or put highly pilferable or sensitive items in a secure place while teleworking and while on travel.
- Promptly report the loss, theft, damage, or disappearance of property to their immediate supervisor.⁷

⁴ GSA directives applicable to protection of property and sensitive information include, but are not limited to: GSA Order 2104.1A CIO, GSA Information Technology (IT) General Rules of Behavior; GSA Order 2180.1 HCO, Rules of Behavior for Handling Personally Identifiable Information (PII); and GSA Order 7800.12 ADM, Management of the U.S. General Services Administration's (GSA) Internal Personal Property.

⁵ "Countdown to Downtown, 1800 F Making Our Move," retrieved from GSA's intranet site, InSite, July 23, 2014.

⁶ "Peds" are short for mobile pedestal filing cabinets on wheels, often used for under desk storage.

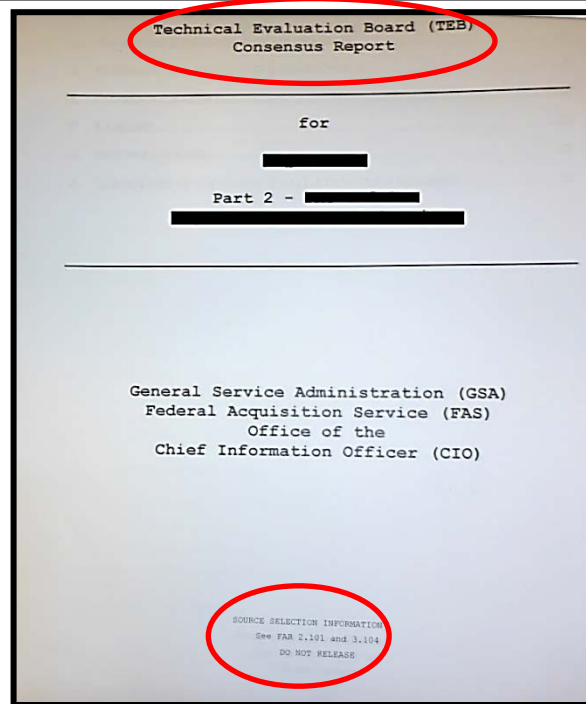
⁷ "Employee Accountability for GSA Property," and "Accountability for GSA Personal Property," certification items (1)(a) through (d), retrieved from GSA's cloud computing environment, August 1, 2014.

FINDINGS

UNSECURED SENSITIVE DOCUMENTS

During the inspection, we observed and documented unlocked personal lockers, drawers, and shared file cabinets that contained PII and other sensitive information. We found unsecured contract files, some containing source selection information marked with strict control designations, as well as personnel and training forms containing PII, a certification of an employee's background investigation, and employee performance appraisals.

Figure 1: Documents such as this labeled “Technical Evaluation Board,” “SOURCE SELECTION INFORMATION,” and “DO NOT RELEASE” were found in unsecured drawers.



We also found keys to cabinets stowed in open personal drawers, allowing anyone to easily gain access to other secured cabinets which could potentially leave more documents vulnerable.

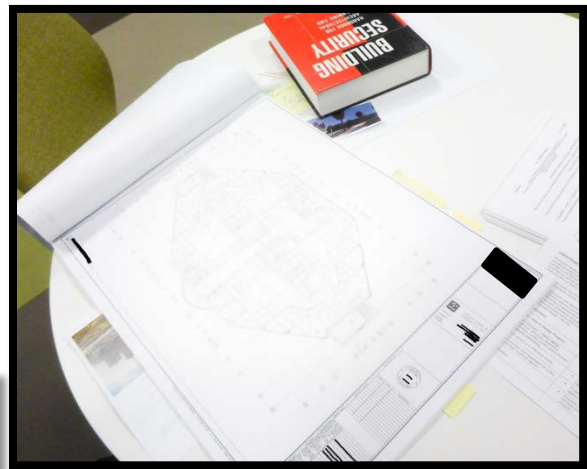
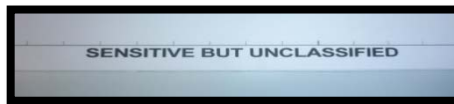
Numerous documents containing PII, such as employee personnel documents, travel vouchers, and *Authorization, Agreement and Certification of Training* (SF-182) forms were found on top of desk surfaces in plain sight.

Figure 2: This folder, labeled “CONFIDENTIAL – OPEN BY ADDRESSEE ONLY,” was found on top of a desk drawer along with other documents. The folder’s seal was broken and contained sensitive employee performance reviews and assessments.



Other sensitive documents were stacked on top of shared working areas. These items contained either PII or other sensitive information. For example, architectural drawings for courthouses and other federal buildings were left unsecured on large tables. These architectural drawings explicitly stated that the information was “SENSITIVE BUT UNCLASSIFIED.” Furthermore, the cabinets designed specifically for holding these large documents did not have locks. In another instance, the combination code for a bay of personal lockers was left directly on top of those lockers. When tested, the combination opened several lockers, one of which contained PII.

Figure 3: Architectural drawings, marked with strict control designations, were left on top of tables. Many were drawings of federal buildings such as courthouses.



The inspection team also found two documents containing employee PII, such as name, address, Social Security number, and phone number, in a shared supply center. One document was found in a printer tray, while the other was stacked in a tray designated for printing jobs that had not been retrieved. GSA Rules of Behavior for Handling Personally Identifiable Information (PII) explicitly states “Don’t let PII documents sit on a printer where unauthorized employees or contractors can have access to the information.”⁸

⁸ GSA Order 2180.1 HCO, GSA Rules of Behavior for Handling Personally Identifiable Information (PII) section (7)(i).

The GSA Information Technology (IT) Security Policy (CIO P 2100.1I) requires employees to report incidents of unsecured documents containing PII to an information security officer, or other proper authorities. After our physical inspection, we contacted the GSA Privacy Officer to inquire about employee reports of PII breaches at the GSA Central Office. We were advised of one reported breach within the last year.

During the inspection, items that were sensitive and unsecurable were removed, and a notice was left stating, “We identified unsecured sensitive information. Due to the sensitive nature of this information, we have taken possession of it to secure its privacy,” and included our contact information for retrieval. Many employees who contacted our office to retrieve these unsecured sensitive items had no knowledge of exactly what items were taken from their work spaces. Some items have yet to be claimed.

UNSECURED HIGHLY PILFERABLE PERSONAL PROPERTY

During our inspection, an HSPD-12 PIV card was found in an unsecured drawer. The badge belonged to a former GSA contractor. We tested the badge on the security turnstile and found it to be active. An active HSPD-12 PIV permits unrestricted physical access to the GSA Central Office building, and potentially any federal building. This indicates inadequate security over HSPD-12 processing and raises further questions as to GSA’s procedures for confiscating or deactivating HSPD-12 cards that should no longer be in use. As of the date of this report, no one has contacted the OIG to claim the badge, and the building security office has advised that there have been no reports of this HSPD-12 card being missing, lost, or stolen. The OIG is currently addressing this issue through the ongoing review, *Evaluation of Controls over HSPD-12 Issuance and Destruction for Contractors*.

Figure 4: This HSPD-12 PIV card was found in an unsecured drawer.

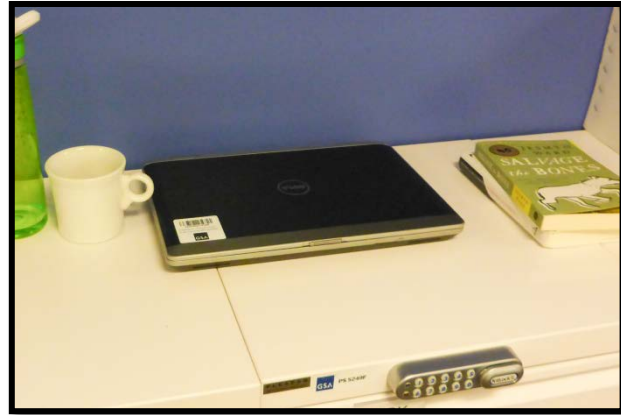


In addition, we found a GSA issued laptop that was left on top of a bay of lockers. During the inspection, we were unable to determine which employee it was assigned to, or which locker it should have been secured in. Consequently, we took possession of it, and inventoried it with the other items that we secured.

The owner contacted us and was able to pick it up the next day. Upon retrieving the confiscated laptop, the employee explained that both personal possessions and GSA property did not fit into an assigned locker; therefore, the employee had decided to secure personal belongings (several

pairs of shoes) in the locker rather than the GSA laptop. An assessment of the adequacy of secure storage space at the GSA Central Office is needed.

Figure 5: This laptop was left unsecured on top of a bay of lockers.



Many supplies and high-value electronics, such as portable laminate machines and projectors – each valued up to \$1,000 – were found in unlocked closets and were vulnerable to theft. Additionally, we found unsecured laptops in open drawers at multiple peds.

Figure 6: Two laptops were found in an unlocked drawer. These items were secured in place by the OIG inspectors.



Throughout the inspection we observed that supply centers and their related inventory, such as toner cartridges, were accessible after-hours, increasing the risk of theft. Cabinets in the supply centers were easily securable; however, keys were left in their corresponding cabinet locks. We contacted Federal Protective Services (FPS) to determine if there were any reported thefts since the transition into the new shared open office space. FPS advised that in the last year there were five reported thefts at the GSA Central Office, two of which were thefts of GSA property.

CONCLUSION

GSA requires and provides training and guidance to address physical security risks to its employees and contractors. However, the lack of due diligence in safeguarding PII, other sensitive information, and highly pilferable government-furnished personal property, leaves GSA vulnerable to potential threats. As a result of this inspection, the agency has since publicized numerous security reminders in poster displays, emails, and blogs.

RECOMMENDATIONS

1. GSA supervisors and managers should enforce GSA policies and procedures for the safeguarding of PII, other sensitive information, and highly pilferable government-furnished personal property.
2. GSA supervisors and managers should routinely monitor for security compliance by both employees and contractors.
3. GSA supervisors and managers should assess the adequacy of secure storage space available to meet employee and contractor needs.

APPENDIX A – OBJECTIVE SCOPE AND METHODOLOGY

The Office of Forensic Auditing, Evaluation and Analysis performed an unannounced after-hours building inspection of shared open space to identify weaknesses in the physical security of sensitive information and highly pilferable government-furnished personal property. The inspection was conducted in the newly renovated 1800 F GSA building on Wednesday July 30, 2014 between the hours of 7:00 p.m. and 11:00 p.m. EST. The searches we performed for this inspection were limited to the Central Office located at 1800 F Street, NW, Washington, D.C.

We conducted this inspection in accordance with Quality Standards for Inspection and Evaluation developed by the Council of the Inspectors General on Integrity and Efficiency. In accordance with those standards, we planned and performed the inspection to collect sufficient, relevant evidence to provide a reasonable basis for our findings, conclusions, and recommendations.

In order to accomplish the objective, we subjectively selected workstations, office storage, and office rooms in the open work space, including supply centers and conference rooms, to perform targeted searches for: (1) unsecured highly pilferable government-furnished personal property (such as laptops and other electronics); and (2) unprotected sensitive information, including PII.

To perform our test work of certain physical controls over the security of vulnerable assets and sensitive information, we performed a subjective search of GSA open work space. We subjectively selected floors and areas to search, from the basement level to the 7th floor. In order to discover instances of unsecured sensitive information and highly pilferable government furnished property, we conducted the following steps:

- Tested for unlocked cabinets/safes/lockers;
 - Inspected contents of unlocked cabinets/safes/lockers;
- Probed for unlocked computer screen access;
- Searched personal workspaces, supply centers, trash bins, recycle bins, closets, and countertops;
- Scanned for keys and lock combinations, and;
- Tested for unlocked offices.

When unsecured sensitive documentation was encountered, we used our professional judgment to determine whether it required our removal and safeguarding. If sensitive business documents were found in lockable cabinets, we locked the cabinets and confiscated the keys to secure them. Examples of criteria used to confiscate or secure documents included:

- Social Security numbers combined with names, addresses, or other personal information.
- Documents marked Limited Official Use Only (LOUO), sensitive, For Limited Use Only, Sensitive but Unclassified, Do Not Release, Do Not Distribute, etc.

When we encountered unsecured highly pilferable valuable property, we used our professional judgment to determine whether it required our removal and safeguarding. If highly pilferable

valuable property was found in lockers, we secured it by locking it in the passcode-protected electronic lockers.

For all instances when unsecured sensitive information or highly pilferable personal property was removed for safeguarding, as well as all instances when cabinet keys were confiscated, a notice was left at the workspace detailing our action. The notice stated that we had taken possession of the sensitive information to secure its privacy, and included OIG contact information for retrieval.

Because we were unable to remove and safeguard all items documented during the inspection, a memorandum was issued on July 31, 2014 to the Central Office building services manager describing the conditions found and recommending GSA take all necessary action to ensure sensitive information is physically protected in the Central Office open space.⁹

All of our findings are based on observation during our inspection work performed on July 30, 2014. We documented all of our evidence with photographs and detailed descriptions of our findings on each floor. All evidence was approved by the Director of Office of Forensic Auditing, Evaluation and Analysis, who was onsite to supervise the work for the entire span of the inspection. All evidence seized was catalogued for return to its owners. Because of the judgmental nature of the work performed for this inspection, we cannot generalize our results to any other locations or points in time.

⁹ Office of Forensic Auditing, Evaluation and Analysis Memorandum, "GSA Central Office Physical Controls Over Sensitive Information," July 31, 2014.


APPENDIX B – MANAGEMENT COMMENTS



GSA Chief of Staff

October 10, 2014

MEMORANDUM FOR PATRICIA D. SHEEHAN
DIRECTOR, OFFICE OF FORENSIC AUDITING,
EVALUATION AND ANALYSIS (JE)

FROM: ADAM NEUFELD 
CHIEF OF STAFF (AC)

SUBJECT: Response to Draft Report: "Security Vulnerabilities - Protecting
Information and Property in the GSA Central Office Open Space"

I am writing in response to your draft memorandum dated September 29, 2014, concerning the draft report entitled "Security Vulnerabilities—Protecting Information and Property in the GSA Central Open Office Space." Your review identified two issues that warrant our attention: (1) physical control weakness in securing sensitive information covered by the Privacy Act (5 U.S.C. § 552a) and the Trade Secrets Act (18 U.S.C. § 1905); and (2) physical control weakness in securing highly pilferable Government-furnished personal property.

With regard to issue (1), we agree GSA can make improvements to our approach to securing sensitive information. I want to assure you that GSA leadership takes the security of our workplace, as well as the sensitive documents and items we utilize, very seriously. We understand that an open, mobile office may present new challenges to how we secure our space, but we have taken steps to ensure that our employees are aware of how important security of information and property is to our work and our agency.

Since the report from the IG's office, the Office of Communications and Marketing (OCM) launched an extensive campaign targeted at educating the staff on the mandatory policies and procedures that allow us to effectively maintain the integrity of our office.

To date, the agency has sent 10 emails to managers and staff, posted 14 articles on GSA Insite, and held conversations on Chatter. Posters and signage have been placed throughout the building, at desks, by entrances, and near the elevators. GSA has printed and distributed 200 placards at workstations around the building.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

These communications have focused on issues ranging from securing personal documents to properly storing laptops to reminding employees to not forget their PIV (personal identity verification) cards. We have communicated the need to protect sensitive information through GSA newsletters and blogs, as well as messages from Deputy Administrator Denise Roth and other GSA leaders. In addition, we are currently working with GSA IT to implement a message that displays on all computers, reminding employees to properly store their laptop and sensitive materials.

We will continue our communications in support of this effort through additional emails and posts on InSite, as well as an ongoing dialogue with managers about the importance of maintaining the security and integrity of our open office space.

With regard to issue (2), we also are committed to improving upon the physical controls and protocols already in place for securing highly pilferable Government-furnished personal property. We will take a number of actions to ensure all staff are complying with securing Government-furnished personal property. The Office of Administrative Services (OAS) is informing all employees of their responsibilities for GSA personal property through the annual Accountability for GSA Personal Property Rules of Behavior, which delineates the rules and regulations surrounding our use of personal property. As part of this certification, employees must certify that they have read and understand the Rules of Behavior, which are included in an Online University training module. Records of the results of the training are maintained within the OLU system.

Secure operational file storage is readily available throughout 1800 F. During the Needs Assessment process prior to final occupancy, each organization identified their filing requirements and were provided with the requested amount of file storage space. A recent analysis of these storage units indicate that they are only 60 to 70 percent utilized, on average. OAS will review filing requirements with each organization to ensure that they have access to the required secure file management resources. Employees will be advised again of the availability of these storage units.

Lastly, as OAS 1800 F Tenant Support staff perform their duties, they will perform periodic spot checks of workstations and, if they notice a situation which may present an information security issue, they will bring that to the attention of the person at the workstation and OAS leadership, if necessary, so that appropriate corrective action can be taken. Tenant Support staff also monitor public areas, such as supply rooms and copy centers.

If you have any questions, please contact Ms. Cynthia A. Metzler, Chief Administrative Services Officer, at Cynthia.Metzler@gsa.gov 202-357-9697 or me at Adam.Neufeld@gsa.gov 202-208-0785.