OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Sensitive Information at Social Security Administration Offices

A-01-13-13025 | October 2013

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: October 18, 2013 Refer To:

To: The Commissioner

From: Inspector General

Subject: Sensitive Information at Social Security Administration Offices (A-01-13-13025)

The attached final report presents the results of our audit. Our objective was to determine whether sensitive information, such as personally identifiable information, in Social Security Administration offices was at risk for disclosure to the public.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

Sensitive Information at Social Security Administration Offices
A-01-13-13025

October 2013 **Office of Audit Report Summary**

Objective

To determine whether sensitive information, such as personally identifiable information (PII), in Social Security Administration (SSA) offices was at risk for disclosure to the public.

Background

Generally, SSA cannot conduct business without exchanging PII and other sensitive information with the public. PII can be used to distinguish or trace that individual's identity, such as name, Social Security number (SSN), or date of birth.

Safeguarding sensitive information has been a priority for SSA since its creation in 1935. The first regulation the Social Security Board adopted addressed privacy and the disclosure of Social Security records. Subsequent regulations and laws, including the *Privacy Act of 1974*, further defined the Agency's responsibilities to protect sensitive information. Accordingly, the Agency requires that employees protect PII, has established guidance and resources for employees, and annually reminds all employees of that requirement and the availability of those resources.

Our Findings

In April 2013, we made unannounced visits to 38 SSA offices: 24 field offices, 12 hearing offices, and 2 Social Security card centers. During those visits, we either observed or overheard sensitive information at risk in 13 (34 percent) of the 38 offices we visited.

For example, at the front counter area of one field office, we observed a Social Security card (with name and SSN), a letter from SSA to a beneficiary (with their name and address), and a printed application for benefits (with the applicant's name, SSN, and claim-specific information). These documents are common in the daily conduct of business at SSA offices. Additionally, SSA could not control how careful the public was with sensitive information, even though staff remind visitors of the need to be careful.

Conversely, although offices generally were not expecting our visits, we did not observe sensitive information at risk in the remaining 25 offices (66 percent) visited.

Sensitive information, including PII, is at risk for inadvertent disclosure in SSA offices where the public transacts business. Recognizing this, the Agency has taken steps to safeguard sensitive information, including emphasizing to all employees their duty to protect this information and building privacy protections into the physical design of offices.

Our Conclusion

SSA should continue to remind staff on an on-going basis of the importance of protecting sensitive information.

TABLE OF CONTENTS

ABBREVIATIONS

FISMA	*Federal Information Security Management Act of 2002*
PII	Personally Identifiable Information
SSA	Social Security Administration
SSN	Social Security Number

OBJECTIVE

Our objective was to determine whether sensitive information, such as personally identifiable information (PII),[1] in Social Security Administration (SSA) offices was at risk for disclosure to the public.

BACKGROUND

Safeguarding sensitive information has been a priority for SSA since its creation in 1935. The first regulation the Social Security Board adopted addressed privacy and the disclosure of Social Security records. Subsequent regulations and laws, including the *Privacy Act of 1974*,[2] further defined the Agency's responsibilities to protect sensitive information.

Accordingly, SSA (a) requires that employees protect PII, (b) established guidance and resources for employees, and (c) annually reminds all employees of that requirement and the availability of those resources. Additionally, (in response to Office of Management and Budget requirements),[3] SSA employees sign a statement every year acknowledging that they have read and understood the Agency's annual reminder on safeguarding PII.

SSA established field offices, hearing offices, and Social Security card centers for the public to transact business. Generally, SSA cannot conduct business without exchanging PII and other sensitive information with the public. Although designed in a variety of layouts that separate the public from employee work areas, all offices have areas where the public and SSA staff interact. For example, all offices have a reception area where members of the public typically provide an SSA employee with their name and Social Security number (SSN). Some field offices have an employee work area near the reception area where claims representatives interview the public for benefit applications, and members of the public circulate through this area escorted by SSA staff. In other offices, claims representatives conduct benefit application interviews at their desks in the staff work area.

---

[1] PII is ". . . any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." U.S. Department of Commerce, National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122, § 2.1, April 2010, p. 2–1, citing GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008.

[2] *Privacy Act of 1974*, 5 U.S.C. § 552a.

[3] Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.

SSA Safeguards for Sensitive Information

The Agency stresses the importance of protecting sensitive information through a variety of efforts.

- **Training:** SSA teaches privacy as a service principle and core value as one of the first lessons for newly hired employees whose jobs involve direct public contact.[4] Employees may also access video-on-demand training on safeguarding PII.

- **Annual Reminder:** SSA formally reminds all employees each year of their duties and responsibilities under the *Privacy Act* and requires that employees protect PII. The Agency requires that employees who have access to PII sign a statement acknowledging they have read and understood the Agency's annual reminder document on safeguarding PII.

- **Resources:** SSA provides a link to PII resources on the main page of its Intranet site. The Agency maintains multiple online resources for employees to research and reference Agency PII policy and guidance. This includes a Website that provides "one-stop-shopping" for reporting the disclosure of PII; policy related to specific issues, such as email containing PII and disposal of documents containing PII; and links to online training on specific PII-related topics.

- **Special Efforts:** SSA incorporates the safeguarding of privacy as a topic in ongoing training and reminder efforts, such as the information security bulletins issued periodically by the Office of the Chief Information Officer. As part of its "Think Twice First" campaign, SSA has featured PII or privacy-related security topics at least twice since January 2012.[5] Additionally, we observed that some managers made local efforts, such as

  - posting signs in public areas—including near trash bins—reminding the public to safeguard PII;
  - checking trash bins in public areas to remove any PII;
  - removing trash bins in public areas;
  - providing for public use a secure bin for documents to be shredded; and
  - instructing staff to ask members of the public to write down rather than say aloud their SSNs.

[4] Teleservice (800 Number) representatives, service representatives, claims representatives, benefit authorizers, and claims authorizers.

[5] The "Think Twice First" campaign consists of nine reminders throughout the year on Agency policy. It began as a regional initiative in the San Francisco Region, and SSA adopted it nationally in January 2012.

- **Office Design:** SSA designs the public areas of relocated or remodeled offices where staff and customers discuss PII and sensitive information to safeguard the privacy of members of the public.[6] For example, SSA has incorporated such design features as floor-to-ceiling barrier walls, sound-absorbent material for walls and ceilings, private interview rooms, and the placement of half-walls between the general seating area and interviewing windows in the reception area. However, SSA stated that the availability of financial resources—both in terms of funds to spend on property redesign and the Agency's ability to replace staff lost to attrition who oversee SSA facilities—has resulted in an incremental approach to designing for privacy. Typically, the Agency reassesses privacy concerns as part of the leasing process—generally 2 years before a lease expires. In the past, some field offices have used recorded background noise (such as ventilation system sounds) to help mask conversation that might be overheard.

- ***Ad hoc* Reminders:** SSA field office managers told us that whenever they became aware of a concern—in response to a specific incident, for example—management reminds staff to be vigilant in safeguarding sensitive information.

SSA Offices We Visited

We made unannounced visits to 38 offices in 9 of SSA's 10 regions.[7] Specifically, we visited 24 field offices, 12 hearing offices, and 2 Social Security Card centers located near an Office of the Inspector General, Office of Audit office. We visited all offices during the hours they were open to the public, and we discussed our observations with office management before concluding our visit. See Appendix A for additional information on our scope and methodology. The results presented in this report are a snapshot of what we found in specific SSA offices we visited on certain days in April 2013.

[6] Employee safety is a key concern in certain design elements such as floor-to-ceiling barrier walls.

[7] We did not visit any offices in the Seattle Region because we do not have audit staff there. See Appendix B for a list of offices visited.

RESULTS OF REVIEW

We either observed or overheard sensitive information at risk in 13 (34 percent) of the 38 offices we visited.[8] Although offices generally were not expecting our visits, we did not observe sensitive information at risk in the remaining 25 (66 percent) offices we visited. See Table 1.

Table 1: Results of Visits

TYPE OF SSA OFFICE	NUMBER OF OFFICES VISITED	NUMBER OF OFFICES WHERE WE OBSERVED OR OVERHEARD SENSITIVE INFORMATION	NUMBER OF OFFICES WHERE WE DID NOT OBSERVE OR OVERHEAR SENSITIVE INFORMATION
Field Offices	24	11	13
Disability Adjudication and Review Hearing Offices	12	2	10
Social Security Card Centers	2	0	2
TOTALS	**38**	**13**	**25**

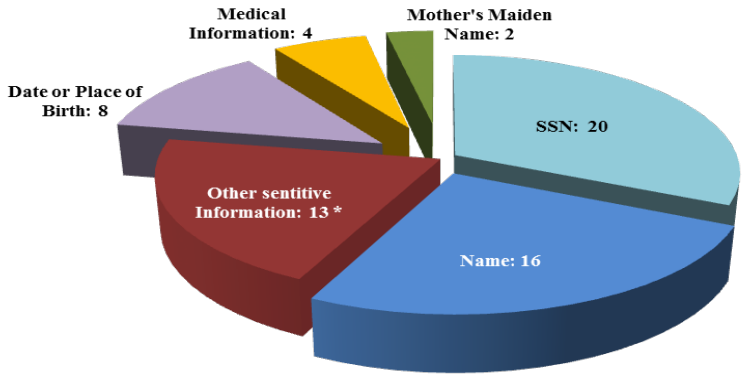
For example, at the front counter area of one field office, we observed a Social Security card (with name and SSN), a letter from SSA to a beneficiary (with their name and address), and a printed application for benefits (name, SSN, and claim-specific information). These are all documents common in the daily conduct of business at SSA offices.

Additionally, SSA could not control how careful the public was with sensitive information. For example, in one hearing office, a conference room available for the use of the claimants and their representatives contained a computer. When the room was not in use, we observed sensitive information on the computer screen that included medical information, as well as the individual's name, SSN, and date or place of birth. The manager stated that staff frequently reminded visitors of the need to be careful.

Figure 1 shows the types and amount of sensitive information we found at risk in 13 of the 38 offices visited.

[8] Although we observed sensitive information at risk, nothing came to our attention to indicate any members of the public actually misused any PII.

Figure 1: Types and Amount of Sensitive Information at Risk



* Other sensitive information included financial and employment information, four incidents each; addresses, two incidents; one incident of educational information; one benefit claim application; and benefit claim information for one interview.

Although the Agency's efforts to create a culture of safeguarding PII has not entirely eliminated the risk of inadvertent disclosure, SSA has established policy and taken action to protect sensitive information from being put at risk. For example, as of May 2013, the Agency stated it had installed barrier walls in about 670 (54 percent) of its approximate 1,250 field offices.

At several offices, management described special efforts it took to safeguard sensitive information. For example, one office kept small document shredders near the front counter so employees could immediately shred no-longer needed documents with PII, rather than piling them up to take later to a large shredder or collection bin elsewhere in the office. Other offices have placed posters in public areas to remind the public to be careful with sensitive information (although they still sometimes find sensitive information carelessly discarded). One office, knowing this to be a common occurrence, routinely sent a supervisor into public areas specifically to search for discarded PII.

CONCLUSION

Sensitive information, including PII, is at risk for inadvertent disclosure in SSA offices where the public transacts business with the Agency. Recognizing this, the Agency has taken a number of steps to safeguard sensitive information, including emphasizing to all employees their duty to protect this information and building privacy protections into the physical designs of offices. SSA should continue to remind staff on an ongoing basis of the importance of protecting sensitive information.

AGENCY COMMENTS

SSA reviewed the draft report but did not provide any comments. See Appendix C.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objective, we conducted unannounced visits to 38 Social Security Administration (SSA) offices that the public could visit to conduct business. We visited the offices during the hours they were open to the public on Tuesday, April 23, 2013; Wednesday, April 24, 2013; or Friday, April 26, 2013.

Rather than randomly select the offices we visited, we selected offices located near an Office of the Inspector General, Office of Audit office. Specifically, we visited

- 24 field offices,
- 12 hearing offices, and
- 2 Social Security card centers.

At the SSA offices, we walked through areas accessible to the public and noted personally identifiable information (PII) that a member of the public might see or overhear. We discussed the results with SSA management at the conclusion of each visit.

We obtained information from SSA regarding office redesign and privacy protection and obtained and reviewed SSA policies and procedures related to safeguarding PII.

The entities audited were field offices and Social Security card centers under the Office of the Deputy Commissioner for Operations and hearing offices under the Office of the Deputy Commissioner for Disability Adjudication and Review. Also, the *Federal Information Security Management Act of 2002 (FISMA)* requires that the Agency's Chief Information Officer ensure compliance with FISMA, which encompasses efforts to safeguard PII.[1] We conducted this performance audit 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 findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] *FISMA*, § 301, § 3544(a)(3), 44 U.S.C. § 3544(a)(3).

Appendix B – Offices Visited

Table B–1: Offices Visited

TYPE OF OFFICE	CITY AND STATE	SSA REGION
Field Office	Fitchburg, Massachusetts	Boston
Field Office	Gardner, Massachusetts	Boston
Field Office	Quincy, Massachusetts	Boston
Field Office	Manchester, New Hampshire	Boston
Hearing Office	Manchester, New Hampshire	Boston
Field Office	Providence, Rhode Island	Boston
Hearing Office	Providence, Rhode Island	Boston
Field Office	Hoboken, New Jersey	New York
Hearing Office	New York, New York (Manhattan)	New York
Social Security Card Center	New York, New York, (Manhattan)	New York
Field Office	Union, New Jersey	New York
Field Office	Baltimore, Maryland	Philadelphia
Field Office	Owings Mills, Maryland	Philadelphia
Field Office	Philadelphia, Pennsylvania	Philadelphia
Hearing Office	Philadelphia, Pennsylvania	Philadelphia
Social Security Card Center	Philadelphia, Pennsylvania	Philadelphia
Field Office	Washington, District of Columbia	Philadelphia
Hearing Office	Washington, District of Columbia	Philadelphia
Field Office	Atlanta, Georgia	Atlanta
Field Office	Atlanta, Georgia	Atlanta
Hearing Office	Atlanta, Georgia	Atlanta
Field Office	Bessemer, Alabama	Atlanta
Hearing Office	Birmingham, Alabama	Atlanta
Field Office	Trussville, Alabama	Atlanta
Field Office	Chicago, Illinois	Chicago
Field Office	Chicago, Illinois	Chicago
Hearing Office	Chicago, Illinois	Chicago
Field Office	Dallas, Texas	Dallas
Hearing Office	Dallas, Texas	Dallas
Field Office	Kansas City, Missouri	Kansas City
Hearing Office	Kansas City, Missouri	Kansas City
Field Office	Lenexa, Kansas	Kansas City
Field Office	Denver, Colorado	Denver
Hearing Office	Denver, Colorado	Denver
Field Office	Berkeley, California	San Francisco
Hearing Office	Oakland, California	San Francisco
Field Office	Richmond, California	San Francisco
Field Office	Walnut Creek, California	San Francisco

Appendix C – AGENCY COMMENTS

September 17, 2013

Subject: Audit No. 22013043 - OIG Draft Report, "Sensitive Information at Social Security Administration Offices"

Steve,

Thank you for the opportunity to review the Office of the Inspector General draft report, *Sensitive Information at Social Security Administration Offices*. We agree with the report as written and offer no comments.

Please let me know if you have any questions.

Tina

Tina M. Waddell
Assistant Deputy Commissioner
for Budget, Finance and Management

Appendix D – Major Contributors

Judith Oliveira, Director

David Mazzola, Audit Manager

David York, Program Analyst

Brennan Kraje, Statistician

Additionally, Office of Audit staff nationwide conducted the office visits.

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (http://oig.ssa.gov/) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "Beyond The Numbers" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.


Watch us on YouTube


Like us on Facebook


Follow us on Twitter


Subscribe to our RSS feeds or email updates

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at http://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at http://oig.ssa.gov/e-updates.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website:	http://oig.ssa.gov/report-fraud-waste-or-abuse
Mail:	Social Security Fraud Hotline P.O. Box 17785 Baltimore, Maryland 21235
FAX:	410-597-0118
Telephone:	1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
TTY:	1-866-501-2101 for the deaf or hard of hearing