OFFICE OF THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

CONTROLS OVER THE FLEXIPLACE PROGRAM AND PERSONALLY IDENTIFIABLE INFORMATION AT HEARING OFFICES

June 2010 **A-08-09-19079**

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.
- Promote economy, effectiveness, and efficiency within the agency.
- Prevent and detect fraud, waste, and abuse in agency programs and operations.
- Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.

To ensure objectivity, the IG Act empowers the IG with:

- Independence to determine what reviews to perform.
- Access to all information necessary for the reviews.
- Authority to publish findings and recommendations based on the reviews.

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: June 9, 2010 Refer To:

To: The Commissioner

From: Inspector General

Subject: Controls over the Flexiplace Program and Personally Identifiable Information at Hearing Offices (A-08-09-19079)

OBJECTIVE

Our objective was to assess controls over the Flexiplace program (Flexiplace), including personally identifiable information (PII), at Office of Disability Adjudication and Review (ODAR) hearing offices.

BACKGROUND

ODAR's hearing offices conduct due-process hearings and issue decisions on appealed determinations involving Old-Age, Survivors and Disability Insurance and Supplemental Security Income. ODAR employs over 1,300 administrative law judges (ALJ) and more than 6,000 support staff, which includes attorney advisors, paralegals, and legal assistants. Among other duties, ODAR support staff conducts initial case screening/preparation and pre-hearing case analysis, develops additional evidence, and prepares notices and decisions for claimants.

Negotiated agreements between the Social Security Administration (SSA) and its unions established Flexiplace for ODAR bargaining unit employees.[1] Flexiplace allows qualified hearing office staff to perform assigned work at a management-approved alternate duty station (ADS), which is typically their personal residence. As such, employees who participate in Flexiplace take claimants' case files to their ADS. These case files can be in paper form or stored on portable devices, such as compact discs (CD) and laptop computers,[2] and generally include claimants' PII—Social Security numbers (SSN), names, addresses, earnings information, and medical histories.

[1] Employees we interviewed were represented by the International Federation of Professional and Technical Engineers, National Treasury and Employees Union, and American Federation of Government Employees.

[2] Hearing office employees we interviewed, other than legal assistants, generally stored claimant case file information on CDs.

According to an ODAR survey, approximately 2,037 (29 percent) of its 6,992 employees worked Flexiplace at least 1 day per week in Calendar Year 2008.[3]

SSA requires that employees who participate in Flexiplace sign, and abide by, the negotiated Flexiplace Program Agreement. While Flexiplace Program Agreements vary depending on the union and/or job position, they share certain basic requirements. For example, SSA requires that Flexiplace employees adhere to all applicable Agency policies and procedures. As such, SSA holds Flexiplace employees accountable for safeguarding Agency records and any PII in their possession.

To accomplish our objective, we selected 20 hearing offices. At each office, we randomly selected and interviewed hearing office employees who participated in Flexiplace in Calendar Year 2008 as well as group supervisors. We also interviewed each office's director and chief ALJ. In total, we interviewed 135 hearing office employees[4] and 75 managerial staff.[5] The scope of our review involved ODAR employees working Flexiplace. Therefore, we did not examine ODAR practices for employees who remove case files to temporary duty sites, such as remote hearing locations. See Appendix B for additional information on our scope and methodology.

RESULTS OF REVIEW

While SSA had implemented some preventative measures to safeguard PII removed from its premises, we determined ODAR practices may have exposed claimant data to unauthorized disclosure. For example, ODAR allowed employees to remove PII stored on unencrypted[6] CDs. In addition, ODAR employees did not always comply with SSA's preventative controls, such as locking claimant PII, when traveling to, or working at, an ADS. We also determined that ODAR did not always identify the removal, and confirm the return, of PII. We believe ODAR should identify opportunities to better monitor employee compliance and strengthen Flexiplace controls, where practicable.

According to most ODAR employees we interviewed, SSA's Flexiplace program has had a positive impact on their morale or helped them work more effectively at home because of fewer interruptions. While we are pleased to report these results, we also recognize there are inherent risks in the Flexiplace program because some

[3] We obtained these numbers from ODAR's Calendar Year 2008 Region-Wide Telework Survey and SSA's Office of Human Resources, respectively. The 6,992 figure includes both regional and hearing office employees. We did not determine whether each employee participated in Flexiplace for the full year.

[4] We randomly selected 136 employees to interview. However, one ALJ declined to participate in our review.

[5] Managerial staff included chief ALJs, hearing office directors, and group supervisors. Although chief ALJs can participate in Flexiplace, we treated them as managerial staff because they are responsible for certain administrative issues concerning ALJs in their offices.

[6] Encryption is one method used to achieve security for data stored electronically. Encryption software converts data into a secret code so they are not easily understood, except by authorized users.

vulnerabilities are outside SSA's control. That is, SSA has limited ability to control or detect how employees transport, store, or use PII when they work Flexiplace. As such, the Agency is at risk for unauthorized disclosure or intentional misuse of claimant PII and must weigh risks against costs and benefits before implementing additional controls.

ODAR'S PRACTICES DID NOT ADEQUATELY SAFEGUARD CLAIMANT DATA REMOVED FOR FLEXIPLACE

ODAR's practices over PII did not properly protect claimant data that Flexiplace employees removed. For example, ODAR management at 17 (85 percent) of the 20 hearing offices we visited allowed Flexiplace employees to remove electronic PII that was stored on unencrypted CDs. As long as employees placed claimants' electronic data in a locked container, ODAR considered the employees to be taking proper steps to secure PII. However, we do not believe such controls are sufficient because PII remains vulnerable to unauthorized disclosure when it is "secured" in such ways.

The Office of Management and Budget (OMB) requires that Federal agencies encrypt all data on mobile computers/devices, unless the data are not sensitive.[7] To address OMB's requirement, SSA implemented a policy that requires employees use Agency-approved encrypted or password-protected electronic devices when PII is removed in electronic form.[8] If device encryption is not possible, SSA requires that employees encrypt or password-protect the electronic files.[9] However, the Agency's current encryption process is incompatible with the computer application[10] ODAR uses for electronic claimant records. In addition, ODAR staff we interviewed told us they could not password-protect electronic files saved to CDs. While SSA is working on an encryption solution for ODAR, we believe ODAR needs to adequately safeguard claimants' electronic data by requiring that employees save PII to an encrypted and password-protected laptop—at least until the Agency implements a complete encryption solution.

We realize storing electronic PII on password-protected laptops will not diminish all risks in the Flexiplace program. However, three hearing offices we visited recognized the vulnerability of employees removing PII on unencrypted CDs and no longer allow employees to remove CDs for Flexiplace.

---

[7] OMB, M-07-16, Attachment 1 § C., May 22, 2007.

[8] SSA, *Safeguarding Personally Identifiable Information (PII) While in Electronic or Physical Transit or Outside of Secure SSA Space*, page 3, February 21, 2008.

[9] Id.

[10] ODAR's computer application, eView, enables employees who process claimants' disability cases to view the information in electronic form.

FLEXIPLACE EMPLOYEES DID NOT ALWAYS COMPLY WITH AGENCY POLICIES WHEN REMOVING PII FROM THE WORKPLACE

ODAR employees did not always adequately secure or properly safeguard PII when working Flexiplace. While SSA has limited capabilities to reduce inherent risks in Flexiplace, it has implemented policies and directives to minimize the opportunity for unauthorized disclosure. For example, SSA requires that employees make every reasonable effort to secure and lock PII and electronic devices during transport and at their ADS.[11] SSA also requires that employees self-report the disposal of PII at their ADS to their managers.[12] Managers must then ensure these employees destroyed PII in an SSA-approved manner.[13]

We determined that 5 (about 4 percent) of the 135 hearing office employees interviewed placed case file information, which contained PII, in an unlocked case or envelope when traveling. We also learned that employees did not always secure PII while at their ADS. For instance, employees told us they placed PII in a travel bag, bookcase, or in their basement instead of locking it in a drawer or cabinet. In fact, 5 (about 4 percent) of the 135 employees we interviewed believed that "locking the house" was adequate protection. Moreover, we learned that an employee left claimant files containing PII in a car overnight. Later, he discovered that someone had broken into his garage and stolen his car. Fortunately, the car and files were recovered, and it appeared there was no disclosure of sensitive data. Additionally, we learned that four employees shredded documents[14] or CDs that contained PII at their ADS, but their managers had not approved the disposals.

We recognize that SSA's PII policies and procedures can only be effective if employees strictly adhere to them. Further, we believe it is SSA's responsibility to protect claimants' PII, to the maximum extent possible, from unauthorized disclosure. Accordingly, SSA should reemphasize to its employees the importance of understanding and following all PII policies and directives. In addition, SSA should take disciplinary action, such as suspending Flexiplace, for those employees who do not comply with its PII requirements.

---

[11] SSA, *Safeguarding Personally Identifiable Information (PII) While in Electronic or Physical Transit or Outside of Secure SSA Space*, Supra at page 2.

[12] Id.

[13] SSA, *Safeguarding Personally Identifiable Information (PII)*, pages 1, 2, and 5, February 14, 2008.

[14] The employees told us these documents were not originals—that is, the employees created the documents specifically for Flexiplace work.

ODAR COULD STRENGTHEN CONTROLS FOR TRACKING PII REMOVED FOR FLEXIPLACE

While Agency policy requires that management closely monitor employee removal of PII from its premises,[15] we do not believe ODAR's practice always confirmed Flexiplace employees' removal and return of PII. SSA requires that management maintain a tracking log to identify PII that employees take to an ADS.[16] ODAR's logs generally include the employee's name, claimant's name and SSN, reason for the PII removal, and dates removed and returned. However, most hearing offices we visited did not track the *type* of medium containing PII that employees removed. In addition, instead of physically confirming that employees returned PII—that is, their CDs, laptops, or paper files—ODAR managers often relied on employees' completed log sheets or case status in its Case Processing and Management System.[17]

We believe ODAR has the opportunity to strengthen its controls for tracking PII. In fact, we determined that one hearing office's group supervisor accounted for electronic PII his employees removed. The group supervisor told us he personally provided CDs to Flexiplace employees and required that they bring the CDs to him upon their return to work.

We recommend that SSA consider establishing additional procedures to identify and account for media that ODAR employees take to their ADS. For example, ODAR's tracking log could include the *type* of medium removed. In addition, ODAR managers could verify that Flexiplace employees physically returned the medium containing the PII.

SSA SHOULD SEEK OPPORTUNITIES TO BETTER MONITOR ODAR EMPLOYEES' COMPLIANCE WITH PII REQUIREMENTS

We believe SSA should improve monitoring of ODAR employees' compliance with Flexiplace requirements and seek opportunities to reduce risks of unauthorized disclosure of PII. For example, SSA could require that ODAR periodically verify that Flexiplace employees place claimant files in a locked container before they travel to an ADS. SSA could also determine whether deterrent controls, such as ADS inspections,[18] would enhance ODAR employees' compliance. Although inspecting ADSs cannot assure SSA that ODAR employees will properly secure claimant PII when at their ADS, it will confirm their ADS is equipped with a lockable device. During our review, we found that 11 (55 percent) of the 20 hearing offices we visited inspected employees' ADSs.

---

[15] SSA, Information Systems Security Handbook, Chapter 22, § 22.4.

[16] SSA, *Safeguarding Personally Identifiable Information (PII) While in Electronic or Physical Transit or Outside of Secure SSA Space*, Supra at page 2.

[17] ODAR's Case Processing and Management System is a Web-based system that allows management to determine, among other things, the current status of each case.

[18] ODAR employees' Flexiplace Program Agreements allow management to conduct ADS inspections.

Employee transportation and storage of claimant data for Flexiplace presents unique challenges—and additional controls will not diminish all risks related to unauthorized disclosure or intentional misuse of claimant PII. However, we believe the Agency should seek opportunities to reduce risks and implement compensating controls. In addition, ODAR should take disciplinary action, such as suspending Flexiplace, for those employees who do not comply with SSA's PII requirements.

CONCLUSION AND RECOMMENDATIONS

SSA faces a unique challenge in safeguarding and monitoring sensitive data ODAR employees remove while working Flexiplace. Although SSA implemented certain policies and directives to protect claimant PII removed from its premises, these controls can only be effective if they are adequate and employees comply. We recognize SSA's efforts cannot eliminate all risks. Nonetheless, we believe SSA has a stewardship responsibility to minimize security risks inherent in the Flexiplace program, when feasible, and ensure employee compliance with all PII policies and directives.

Accordingly, we recommend that SSA:

1. Require that ODAR employees store electronic PII on an encrypted and password-protected laptop when working Flexiplace, until such time as a CD encryption solution for ODAR is developed.

2. Reemphasize to ODAR employees the importance of complying with all Agency PII policies and directives.

3. Consider implementing additional procedures to account for the removal and return of PII.

4. Improve monitoring of ODAR employees' compliance with Flexiplace requirements. In addition, ODAR should take disciplinary action, such as suspending Flexiplace, for those employees who do not comply.

AGENCY COMMENTS

SSA generally agreed with our recommendations. The Agency's comments are included in Appendix C.

OTHER MATTERS

Hearing Office Management Needs to Improve Its Maintenance of SSA's 7-B Employee Record Extension Files

We determined that hearing office management did not always comply with Agency policy regarding SSA's 7-B Employee Record Extension File (7-B File) for staff. SSA policy requires that supervisors maintain a 7-B File for each employee.[19] Employee 7-B Files should include approved Flexiplace Requests, performance appraisals,[20] and employee-signed annual acknowledgment statements on Systems Sanctions and Safeguarding PII.[21]

During our review, hearing office management could not locate one employee's 7-B File, while others' 7-B Files were incomplete. We also identified 66 incidences where management either did not retain or did not ensure that employees' current Systems Sanctions and Safeguarding PII acknowledgment statements were in their respective 7-B Files.[22] Additionally, three employees' 7-B Files did not contain their performance appraisals. Moreover, hearing office management did not always retain employees' Flexiplace Agreements or their Agreements were incomplete.

We encourage SSA to take steps to ensure that management properly maintains employees' 7-B Files.

Hearing Office Managers Were Unclear on Retention Period for PII Logs

It appears that hearing office managers were unclear on how long they should retain PII logs. Policy requires that management retain PII logs for 2 years.[23] However, in the

---

[19] SSA, Personnel Policy Manual, Chapter S293_1, § 4.1.2.

[20] SSA, Personnel Policy Manual, Chapter S293_4, Exhibit 1.

[21] The two documents are SSA's *Agency Policy for Systems Access, Table of Penalties for Violations and Acknowledgement Statement by Employees* and *Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees.* SSA, *Security Reminders for Managers*, May 2009, page 3.

[22] Of the 66 incidences identified, 43 pertained to the Safeguarding PII document and 23 concerned the Systems Sanctions document. Some employees' 7-B File did not contain both documents, while others' may have lacked only one of these documents.

[23] SSA, Memorandum, PII Log Disposal – INFORMATION, August 19, 2008, and SSA, Information Systems Security Handbook, Chapter 19, § 19.3 D.

event of PII loss, policy further instructs management to store the logs and information pertaining to the loss, such as the incident report and the Change, Asset, and Problem Reporting System number,[24] for 7 years.[25]

Management at 3 (15 percent) of the 20 hearing offices we visited told us they stored PII logs fewer than 2 years. In fact, one hearing office director told us his office did not maintain a log any longer than what is needed to confirm the file has been returned. He further stated that the office did not maintain PII logs for ALJs.

To ensure the Agency can properly track PII that Flexiplace employees remove, we believe it is important that management maintain PII tracking logs on all who participate in Flexiplace for the time period required. Therefore, we encourage SSA to clarify the retention period for PII logs with hearing office managers.

Patrick P. O'Carroll, Jr.

[24] SSA's Network Customer Service Center assigns a Change, Asset, and Problem Reporting System number when management or staff reports a PII loss. If additional or updated information on the incident becomes available, managers provide the Network Customer Service Center with this number to update the particular case.

[25] Id., and SSA, Information Systems Security Handbook, Appendix V.

Appendices

Acronyms

7-B File	7-B Employee Record Extension File
ADS	Alternate Duty Station
ALJ	Administrative Law Judge
CD	Compact Disc
Flexiplace	Flexiplace Program
ODAR	Office of Disability Adjudication and Review
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SSA	Social Security Administration
SSN	Social Security Number

Scope and Methodology

To accomplish our objective, we:

- Reviewed pertinent sections of the Social Security Administration's (SSA) policies and procedures pertaining to the Flexiplace program (Flexiplace) and safeguarding personally identifiable information (PII).[1]
- Identified the two hearing offices in each region with the highest percentage of Flexiplace participation in Calendar Year 2008 for our site visits.[2] The hearing offices we visited are shown in Table B-1.

Table B-1: Hearing Offices Visited by Region

	Region	Hearing Office Location
1	I	New Haven, Connecticut
2		Portland, Maine
3	II	Voorhees, New Jersey
4		Newark, New Jersey
5	III	Harrisburg, Pennsylvania
6		Seven Fields, Pennsylvania
7	IV	Birmingham, Alabama
8		Paducah, Kentucky
9	V	Detroit, Michigan
10		Oak Park, Michigan
11	VI	Fort Worth, Texas
12		Dallas North, Texas
13	VII	Creve Coeur, Missouri
14		Kansas City, Missouri
15	VIII	Fargo, North Dakota
16		Billings, Montana
17	IX	Stockton, California
18		Phoenix, Arizona
19	X	Seattle, Washington
20		Spokane, Washington

[1] The scope of our review was limited to Flexiplace. As such, we did not examine the Office of Disability Adjudication and Review's (ODAR) controls in place or employees' PII practices at temporary duty sites, such as remote hearing locations.

[2] We obtained this information from SSA's ODAR and Office of Human Resources.

- Randomly selected two employees per position to interview, if there were at least two employees in that position who participated in Flexiplace. We also randomly selected two group supervisors to interview, if there were at least two in the position. We also interviewed hearing office directors and chief administrative law judges (ALJ), provided there was one.[3] Table B-2 provides the number of hearing office employees and management we interviewed. One ALJ declined to participate in our review.

Table B-2: Employees Interviewed Per Position

Position	Number of Employees Interviewed
ALJ	33
Attorney Advisor	35
Paralegal	29
Legal Assistant	38
Total Employees	**135**
Group Supervisor	36
Hearing Office Chief ALJ	19
Hearing Office Director	20
Total Management	**75**
GRAND TOTAL	**210**

- For each employee interviewed, we examined his/her SSA 7-B Employee Record Extension File to identify whether management retained employees' annual acknowledgment statements[4] and Flexiplace documents.

Our review of internal controls was limited to SSA's policies and directives for protecting PII and documenting Flexiplace requests and approvals. We performed our audit at the Office of Audit in Birmingham, Alabama, and selected hearing offices. The data were sufficiently reliable to meet our objective.

The SSA entity audited was the Office of the Chief ALJ under the Deputy Commissioner for ODAR. We conducted this performance audit from May through December 2009 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[3] One hearing office did not have an acting chief ALJ at the time of our review.

[4] The statements are SSA's *Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees* and *Agency Policy for Systems Access, Table of Penalties for Violations and Acknowledgement Statement by Employees*.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: May 24, 2010 Refer To:

To: Patrick P. O'Carroll, Jr.
Inspector General

From: James A. Winn /s/
Executive Counselor to the Commissioner

Subject: Office of the Inspector General (OIG) Draft Report, "Controls Over the Flexiplace Program and Personally Identifiable Information at Hearing Offices" (A-08-09-19079)

Thank you for the opportunity to review and comment on the draft report. We appreciate OIG's efforts in conducting this review. Attached is our response to the report findings and recommendations.

Please let me know if we can be of further assistance. You may direct staff inquiries to Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-4636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "CONTROLS OVER THE FLEXIPLACE PROGRAM AND PERSONALLY IDENTIFIABLE INFORMATION (PII) AT HEARING OFFICES" (A-08-09-19079)

We generally agree with the reported findings and recommendations.

Recently, the Office of Disability Adjudication and Review (ODAR) launched a multi-pronged strategy on PII loss prevention. Specifically, ODAR's Deputy Commissioner personally issued clear PII loss prevention guidance to all ODAR employees and conducted national teleconferences, including calls to over 570 Information Technology (IT) staff and managers, all Regional Chief Administrative Law Judges (ALJ), and an all-manager call with over 650 managers. ODAR also kicked-off a national PII loss prevention workgroup to quickly review and revise our loss prevention procedures and policies and to establish standard penalties for employee and contractor PII loss.

Additionally, ODAR plans to reemphasize the importance of management accountability. For example, ODAR is developing and will soon issue a certification form for all managers to sign, acknowledging that: 1) all personal drives have been examined for PII and that extraneous information has been purged, 2) all employees have a signed and current copy of the *Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees* on file, and, 3) when applicable, all employees have current, signed flexiplace agreements in their 7B file. Also, ODAR's Systems Security Branch, in conjunction with the agency's Office of Human Resources, is developing a stronger PII element for managers' performance plans. This stronger performance element will hold mangers more accountable for protecting PII.

ODAR's managers also regularly exchange PII protection information and best practices. For example, ODAR's Component Security Officer (CSO) chairs a monthly ODAR Security Roundtable meeting which allows Headquarters Security Specialists, the Division of Electronic Services, the Division of Information Technology Integration, Regional Supervisory Information Technology Specialists, and Regional Systems Administrators to exchange information that will enable them to better protect our claimants' PII. Actions from these meetings often include communicating information to regional managers and/or employees.

Finally, ODAR's Systems Security Branch and CSO actively participate in a variety of agency-wide initiatives with the Chief Information Officer's (CIO) PII staff, which include communicating SSA policy to all agency employees. Current initiatives include mandatory PII awareness training and a poster campaign to promote PII awareness**.**

Our responses to the specific recommendations are as follows:

Recommendation 1

We recommend that SSA require that ODAR employees store electronic PII on an encrypted and password-protected laptop when working flexiplace, until such time as a compact disc (CD) encryption solution for ODAR is developed.

Comment

We agree with the first part of your recommendation concerning laptops. We now have an adequate stock of agency-issued, encrypted, password-protected laptops available to employees working flexiplace, and we transfer electronic PII to those laptops for use at employees' alternative duty stations (ADS). As for the second part of your recommendation, we no longer need to develop a "CD encryption solution." We store electronic PII only on approved laptops and no longer remove CDs from the office for flexiplace purposes.

We are taking actions along these lines to protect PII and to phase in a new process. Specifically, we are:

- Reissuing PII policy guidance to reiterate our existing policy that all employees participating in flexiplace must transport electronic PII between the office and their ADS on agency-issued, encrypted, and password-protected laptops.

- Implementing the portable workstation process (PWP) which allows our employees to use their approved laptops as their in-office workstations while connected to our network. While in the office, employees who have PWP download the files they require for flexiplace directly from the network to their laptops. Employees then use those laptops during flexiplace and upload the work that they performed on flexiplace to the network upon their return to the office.

- We have started issuing new laptops with the PWP software, and some employees are using PWP for flexiplace. Until we deploy PWP in all ODAR offices, flexiplace employees who do not have PWP will follow a work-around process and transfer claimants' electronic files to agency-issued, encrypted, and password-protected Universal Serial Bus (USB) flash drives. While still in the office, they will then transfer the files from the flash drive to their approved encrypted, password-protected laptops. We will secure the USB flash drives in our offices, and they will not leave the premises.

Recommendation 2

We recommend that SSA reemphasize to ODAR employees the importance of complying with all Agency PII policies and directives.

Comment

We agree and are taking a number of steps on this front, starting with management accountability. We are developing and will soon issue a certification form that all managers must sign, wherein they acknowledge that:

- All personal drives have been examined for PII and extraneous information has been purged;
- All employees have a signed, current copy of the *Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees* in their 7-B files, and
- Where applicable, all employees have current, signed flexiplace agreements in their 7-B files.

Also, ODAR is developing a stronger PII element for managers' performance plans.

In 2007, we implemented the *Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees*. We are reemphasizing that employees review and understand that document as well as the *Agency Policy for Systems Access*. In addition, ODAR's Systems Security Branch, CSO, and/or Regional Security IT Specialists provide PII security awareness training to all new ODAR employees and managers to ensure that they understand their responsibilities for protecting PII.

We are also taking other actions to raise awareness and protect PII. Specifically, ODAR's Deputy Commissioner personally issued strict PII loss prevention guidance to all ODAR employees. He conducted national teleconferences with more than 570 IT employees and managers and all Regional Chief ALJs. He also held an "all-managers" call with over 650 participants. In addition, ODAR is leading an effort on PII loss prevention to review and revise its loss prevention procedures and policies and to establish standard penalties for employees who lose PII or fail to adhere to agency PII protection policies.

ODAR's managers also regularly exchange PII protection information and best practices. For example, ODAR's CSO chairs a monthly "ODAR Security Roundtable" where key players exchange information to promote better protection of PII; they then communicate this information to regional managers and employees. ODAR also works with other agency components on PII issues. For example, it collaborates with the CIO on a variety of initiatives to raise PII awareness among all agency employees. This includes an initiative for mandatory PII training and a poster campaign to promote PII protection.

Recommendation 3

We recommend that SSA consider implementing additional procedures to account for the removal and return of PII.

Comment

We agree and are improving our controls over the removal and return of PII. We have reemphasized to ODAR managers their responsibilities in this area and have instructed them to modify their logs to include all types of media. This includes paper files (paper is still used to a great extent) and laptops containing PII. As noted under recommendation one, we no longer remove from the office CDs, flash drives, or other types of electronic media for flexiplace purposes.

We are making further strides in this area. For example, ODAR's Division of Security meets regularly to explore other options for improvements and in coming months will be taking other actions such as issuing new logging procedures. We recognize that procedures must be followed consistently, and ODAR is developing business processes to promote that consistency.

Recommendation 4

We recommend that SSA improve monitoring of ODAR employees' compliance with flexiplace requirements. In addition, ODAR should take disciplinary action, such as suspending flexiplace, for those employees who do not comply.

Comment

We agree and have directed our managers to focus their attention on this important task. We are also stressing personal accountability to the employees themselves who participate in flexiplace. In addition, while we already are spot checking flexiplace ADSs, we will examine and revise procedures and adopt a more systematic approach for those efforts. This will include spot checks of employees transporting PII and on-site reviews of ADSs.

As for the disciplinary action you suggest, we already progressively discipline (reprimand, suspension, and removal) employees who do not comply with policies for safeguarding PII. We are developing standard penalties and guidance to more effectively utilize that option where situations warrant. Also, as we note in our comments for recommendation two, we have PII loss prevention managers meetings where we review policies and consider disciplinary actions for situations where an employee looses PII.

OTHER MATTERS

Hearing Office Management Needs to Improve Its Maintenance of SSA's 7-B Employee Record Extension Files

Comment

We agree. We are reissuing guidelines to ODAR managers and directing them to review employees' 7-B files and certify that each contains the appropriate material. We will complete this by June 30, 2010.

Hearing Office Managers Were Unclear on Retention Period for PII Logs

Comment

The ODAR CSO is working with hearing office representatives to review the entire PII logging process, including the procedures for logging PII for flexiplace, PII logs for ALJs, and log retention. Once complete, we will issue updated guidelines to all affected ODAR employees and managers.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kimberly Byrd, Director

Theresa Roberts, Audit Manager

Acknowledgments

In addition to those named above:

Janet Matlock, Senior Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-08-09-19079.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.