
**OFFICE OF
THE INSPECTOR GENERAL**

SOCIAL SECURITY ADMINISTRATION

**THE SOCIAL SECURITY
ADMINISTRATION'S REGIONAL
OFFICE PROCEDURES FOR
ADDRESSING EMPLOYEE-RELATED
ALLEGATIONS IN REGION VI**

March 2004

A-06-03-13075

AUDIT REPORT



Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.



SOCIAL SECURITY

MEMORANDUM

Date: March 8, 2004

Refer To:

To: Horace Dickerson
Regional Commissioner
Dallas

From: Assistant Inspector General
for Audit

Subject: The Social Security Administration's Regional Office Procedures for Addressing Employee-Related Allegations in Region VI (A-06-03-13075)

OBJECTIVE

Our objectives were to evaluate the adequacy of the Social Security Administration's (SSA) policies and procedures for addressing employee-related allegations, determining how well SSA complied with these policies and procedures, and determining whether SSA referred all employee-related allegations that should have been referred to the Office of the Inspector General (OIG).

BACKGROUND

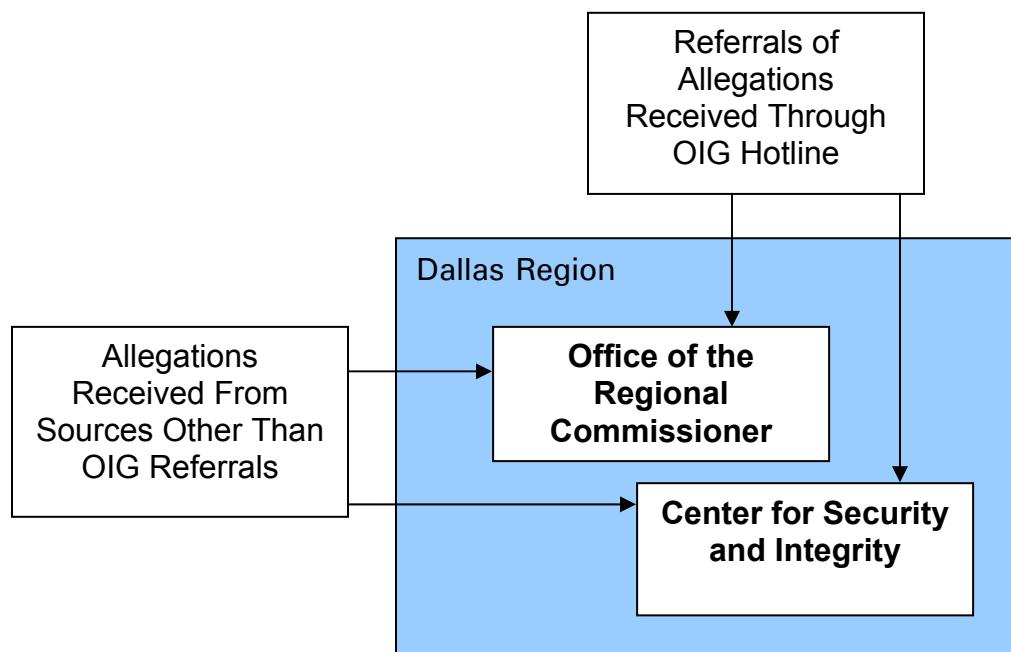
SSA receives various types of allegations related to its programs, the misuse of Social Security numbers (SSN) and employee conduct. Some examples of employee-related allegations include standards of conduct, ethics violations, and the theft of Government property. SSA receives allegations from employees, the public, and the OIG.

Allegations concerning SSA employees are significant because of the potential losses to SSA's programs and the corresponding negative public impact. In determining the validity of allegations, SSA is required to obtain sufficient evidence to support or remove suspicion that criminal violations may have been committed.¹ SSA's policy states:

¹ Program Operations Manual System (POMS), GN 04110.010 A.

"Prior to referral to the Office of the Inspector General, Office of Investigations Field Division, each potential violation and allegation must be developed by the field office, processing center, or other SSA office to the point where enough evidence has been secured to either remove suspicion or substantiate the violation."²

In the Dallas Region, the Office of the Regional Commissioner (ORC) and the Center for Security and Integrity (CSI) review employee conduct and program-related allegations. The ORC reviews all allegations that do not appear to involve fraud. CSI reviews all allegations that appear to involve fraud or employee misconduct that may result in an adverse action. CSI is responsible for supporting field office managers in developing potential fraud issues by using computer system analysis and providing other technical support. Employee allegations that are potential criminal violations must be referred to the OIG for appropriate action.³ Cases involving employee misconduct that are not potential criminal violations are referred to the Center for Human Resources' (CHR) Employee Relations Staff for adverse actions. The ORC and CSI complete workflow processes are illustrated in Appendix C.



In Fiscal Years (FY) 2001 and 2002, OIG referred 37 employee-related allegations to SSA's Dallas Region for action. In addition, the Dallas Region received 70 employee-related allegations from sources other than the OIG.

² POMS, GN 04110.010 B.

³ POMS, GN 04112.005 B.

RESULTS OF REVIEW

SSA's policies and procedures for addressing employee-related allegations were generally adequate; however, we found the following areas need to be addressed.

- The Dallas Region did not refer two potential criminal cases to the OIG for investigation.
- There was inadequate case documentation to support whether allegations were properly resolved for 20 (19 percent) of the 107 allegations.
- The ORC did not retain control logs of allegations received.

We also found management control weaknesses related to accounting for and safeguarding allegation information.

- The ORC's Intranet database did not have adequate safeguards to prevent unauthorized access to employee allegations.
- CSI did not have an adequate allegation tracking system.

NON-COMPLIANCE WITH POLICIES AND PROCEDURES

Referrals to the Office of the Inspector General

We identified 14 allegations that involved a potential employee violation subject to an OIG investigation. Two of the 14 cases were not referred to OIG's Office of Investigations Field Division (OIFD), as required by SSA's policy. SSA policy⁴ states:

“When the evidence and information, *either directly or circumstantially*, establishes that a potential violation may have been committed, forward the allegation to the OIFD. . . . Do not delay forwarding the allegation to the OIFD even if additional information is being developed.”

Both of the allegations involved actions on the list of alleged or suspected employee criminal violations of the Social Security Act, relevant provisions of Title 18 of the United States Code, the Privacy Act of 1974, and conflict-of-interest laws that must be referred to the OIG.⁵ This list is attached as Appendix D.

⁴ POMS, GN 04110.010 C.2.

⁵ POMS, GN 04112.005 A.

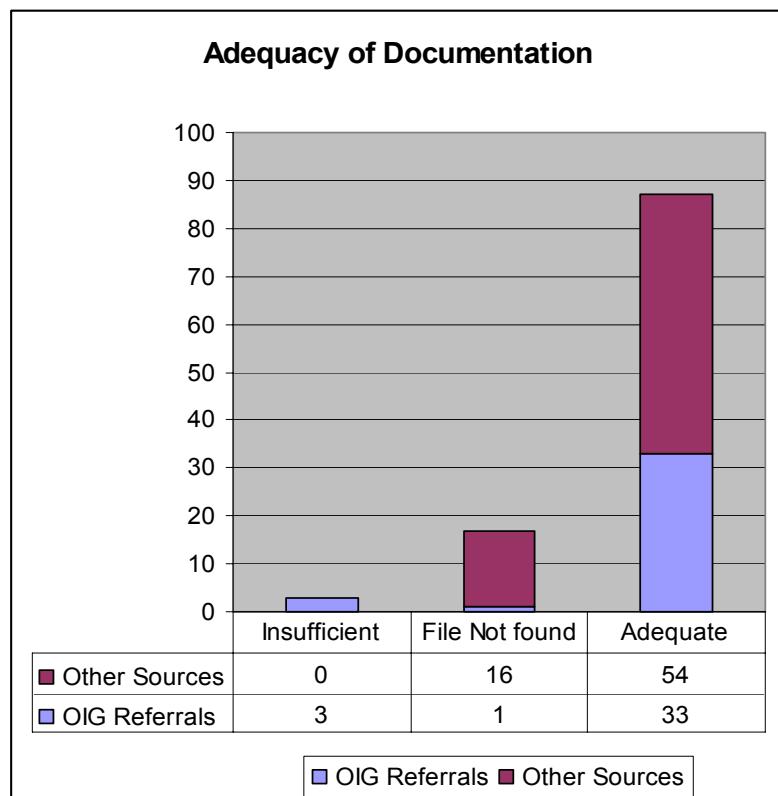
One allegation involved an SSA employee who allegedly completed and signed claimants' signatures on disability determination forms without their knowledge and cleared one overpayment waiver of over \$2,000 without management approval. The SSA field office that identified the employee requested CSI's assistance in obtaining overpayment waivers information to substantiate the suspicions. While the case documentation indicated the field office intended to refer the case to the OIG, and CSI was willing to assist with the referral, neither made the referral. Instead, the case documentation states a letter was sent to the employee with a proposal to remove the employee from service. The employee filed a grievance but decided to take early retirement. CSI was unable to explain why the case was not referred to OIG.

The other allegation involved an employee discarding SSA records without authorization. CHR did not refer the case to the OIG because CHR staff did not consider discarding SSA records a potential criminal action. Our Office of Investigations (OI) informed us that the allegation in question did not rise to the level that would merit a formal criminal investigation. If it were determined, however, that the potential for criminal prosecution did exist, and OI were to conduct a formal investigation, we believe the Department of Justice's willingness to prosecute the case would be diminished in light of administrative/adverse action previously taken by SSA.

Retention of Case Development Documentation

The Dallas Region did not have adequate documentation to either remove suspicion or substantiate the violation, as required by SSA policy, for 20 of the 107 allegations we reviewed. Specifically, 4 of the 37 allegations received from the OIG and 16 of the 70 allegations received from other sources were not properly documented.

For the four cases referred by OIG that did not have adequate documentation, the Dallas Region could not locate one case file, and three case files did not contain sufficient evidence to support whether the allegation was properly resolved.



- In one case, an SSA employee allegedly accessed earnings information from SSA's systems on the records of her ex-spouse and his wife to seek increased child support payments. The case file contained documentation to remove suspicion for accessing one of the SSNs; however, there was no documentation on the second SSN.
- The remaining two cases involved poor customer service. In both cases, there was no evidence in the files that action was taken to determine whether the allegations were properly resolved.

The Dallas Region was unable to locate 16 case files for allegations received from sources other than OIG. All of these cases had been referred to CSI for action and were recorded in its control log. CSI staff informed us that the files had been destroyed to make room for additional files. CSI's control log indicated that most of these allegations involved employees' improper access to SSA's system to query or update a relative's record. CSI's procedures for fraud allegations require that it retain case files for 7 years after the final action is taken.⁶

Retention of Control Logs

The ORC did not have a complete list of allegations received from October 1, 2000 through March 27, 2002. The ORC did not have a complete list because, on March 28, 2002, the ORC began using the Southwest Region Correspondence Control system to track its allegations, and it did not retain its control log from its previous tracking system when it started using the new one.⁷ SSA's policy requires that control logs be retained for 2 years.⁸ Consequently, we were unable to determine whether non-OIG allegations the ORC received were properly controlled, assigned, and resolved.

⁶ CSI, Dallas Region VI, Operating Procedures/Workflow: Employee-related Allegations (FRAUD).

⁷ CSI also did not comply with the record retention requirement. CSI's noncompliance is discussed under the section entitled, *Tracking Allegations Received*, in this report.

⁸ Operational and Administrative Records Schedules, CMS-02.01.00, Control Logs, 09-01-92.

MANAGEMENT CONTROL WEAKNESSES

Access to Sensitive Information

The ORC did not restrict access to its allegations database. The ORC used a web-based system on SSA's Intranet to log all allegations it received for development. The log contained allegations from all sources including the OIG. While there was no apparent link to the web site from SSA's main web page, access to the information was not restricted and could be accessed by anyone who had access to SSA's Intranet. Access to the allegations database should be restricted to authorized individuals. Without restricted access, there is no assurance the allegation data are safeguarded against unauthorized use.

Tracking Allegations Received

Federal regulations prescribe that management controls should ensure access to resources and records is limited to authorized individuals and transactions are promptly recorded, properly classified, and accounted for.⁹ Although CSI used a restricted access electronic database to log the receipt of allegations, the database did not have a field for a sequential control number to track each allegation. A sequential control number would ensure that each allegation is assigned a unique number to properly account for all allegations.¹⁰ At least two allegations were deleted from the log before the required retention period. CSI staff advised us that these cases were probably deleted from the database in an effort to clean up closed cases. Since sequential numbering was not used, there was no trail to alert management of possible unauthorized removal of information. If sequential numbering of entries on the log had been used, when the entries were deleted, there would have been a break in the numerical sequence to alert management of potential tampering of data.

We also found that CSI did not record allegations received from the OIG in a timely manner. CSI recorded allegations in its control log when they were assigned to an analyst for review rather than when they were actually received. When allegations are not logged as received, there is a risk an allegation may not be properly tracked. In one case, the allegation was received from OIG but was never recorded in the control log.

⁹ Office of Management and Budget Circular, A-123, Attachment II, *Establishing Management Controls* (as revised June 21, 1995).

¹⁰ General Accounting Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (11/99).

CONCLUSION AND RECOMMENDATIONS

While SSA's policies and procedures for addressing employee-related allegations were generally adequate, the Dallas Region needs to address identified weaknesses concerning forwarding all potential criminal violations to OIG, documenting evidence, tracking allegations received, restricting access to sensitive information, and complying with record retention requirements.

Accordingly, we recommend the Dallas Regional Office:

1. Ensure allegations with potential employee criminal violations are to be referred to the OIG.
2. Maintain evidence (that is, case development, documentation, and control logs) that supports the clearance of employee-related allegations.
3. Use a password to restrict access to ORC's allegation control log to authorized personnel.
4. Use sequential control numbers for each allegation and record allegations in the control log when received.

AGENCY COMMENTS AND OFFICE OF THE INSPECTOR GENERAL RESPONSE

SSA agreed with all of the recommendations. Regarding recommendation 1, SSA stated that training had been provided to CSI staff to ensure that analysts are properly documenting cases prior to referral to the Employee and Labor Relations Specialist and to officially refer cases with potential criminal violations to OI so that a written declination is part of CSI's file. Concerning recommendation 2, SSA stated that it has now emphasized the need to maintain evidence and added this as a requirement to the CSI workflow procedures. With respect to recommendation 3, SSA stated it is designing a new electronic control file, which will restrict access by authorized employee name, position, and PIN. In the meantime, SSA is applying security measures to the existing control system that will restrict use, based on the user's authority to access the records. Finally, about recommendation 4, SSA stated it now uses sequential control numbers and added that allegations from the Hot Line that come to the component email box will now be logged in and assigned by the Team Leader or Center Director. We believe SSA's response adequately addresses our recommendations and look forward to receiving the corrective action plans. See Appendix E for the full text of SSA's comments.

*Mark S. Stone for
Steven L. Schaeffer*

Appendices

APPENDIX A – Acronyms

APPENDIX B – Scope and Methodology

APPENDIX C – Flowcharts

APPENDIX D – Employee Violations

APPENDIX E – Social Security Administration Comments

APPENDIX F – OIG Contacts and Staff Acknowledgments

Acronyms

CHR	Center for Human Resources
CSI	Center for Security and Integrity
FY	Fiscal Year
OI	Office of Investigations
OIFD	Office of Investigations Field Division
OIG	Office of the Inspector General
ORC	Office of the Regional Commissioner
POMS	Program Operations Manual System
SSA	Social Security Administration
SSN	Social Security Number

Scope and Methodology

We limited our review to Fiscal Years (FY) 2001 and 2002. This included 37 referrals from the Office of the Inspector General (OIG), 70 employee-related allegations from sources other than the OIG, and the 5 potential criminal violation cases identified from the list of adverse actions processed by the Center for Human Resources' (CHR) Employee Relations Staff.

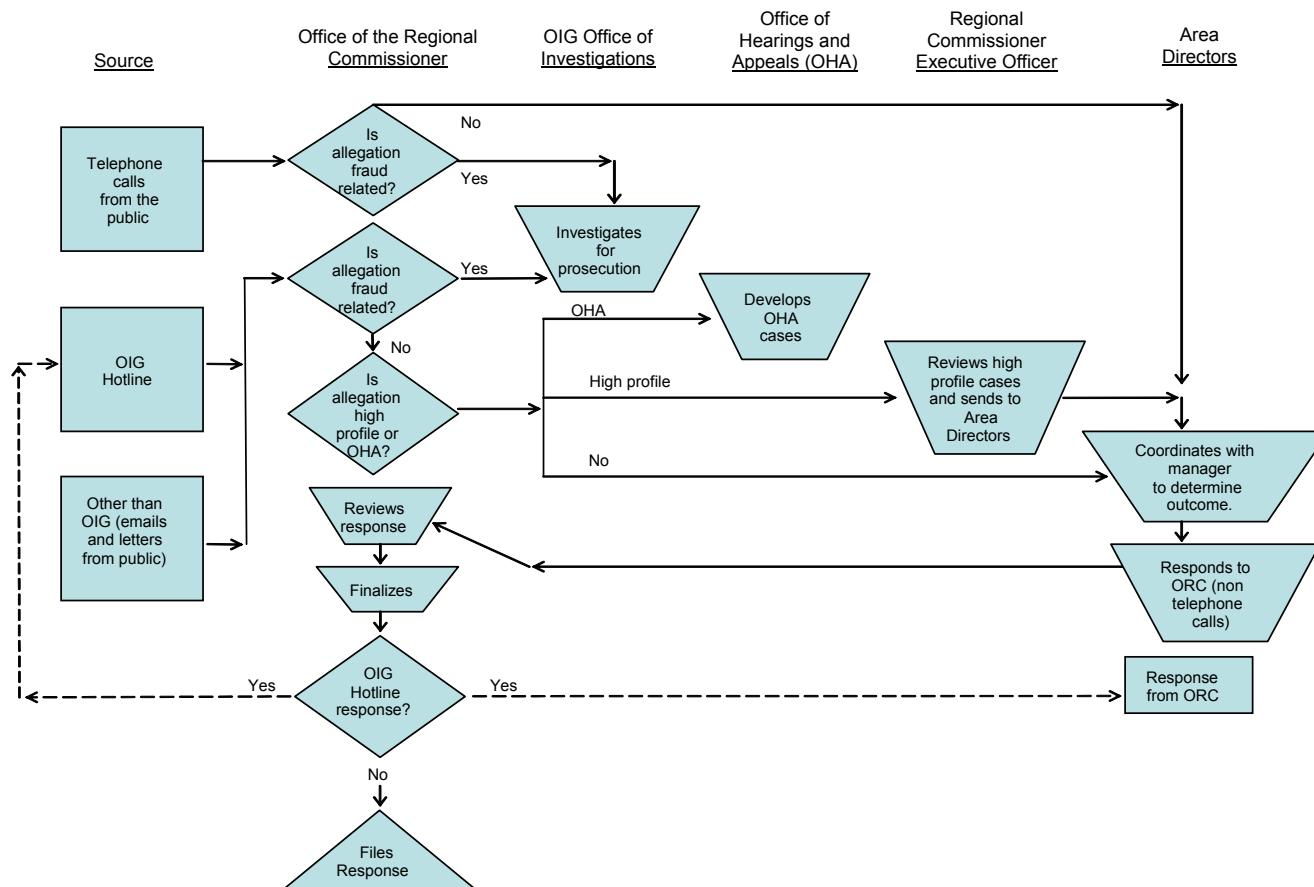
To accomplish our objectives, we:

- Reviewed the following criteria:
 - Office of Management and Budget Circular A-123, *Management Accountability and Control*,
 - Program Operations Manual System,
 - the Social Security Administration's (SSA) Administrative Instructions Manual System,
 - Annual Personnel Reminders, and
 - Standards of Ethical Conduct for Employees of the Executive Branch.
- Obtained the database of allegations processed by the OIG during FYs 2001 and 2002 and identified those listed as employee-related.
- Interviewed officials within the Office of the Regional Commissioner (ORC), Center for Security and Integrity (CSI), and CHR in Dallas, Texas.
- Reviewed ORC and CSI control logs to identify employee-related allegations from sources other than the OIG.
- Reviewed the 97 adverse actions processed by the CHR Employee Relations Staff to identify potential employee-related allegations.
- Reviewed ORC and CSI documentation for the development of evidence related to allegations received from the OIG and other sources.
- Reviewed documentation processed by CHR for the development of evidence applicable to adverse actions.

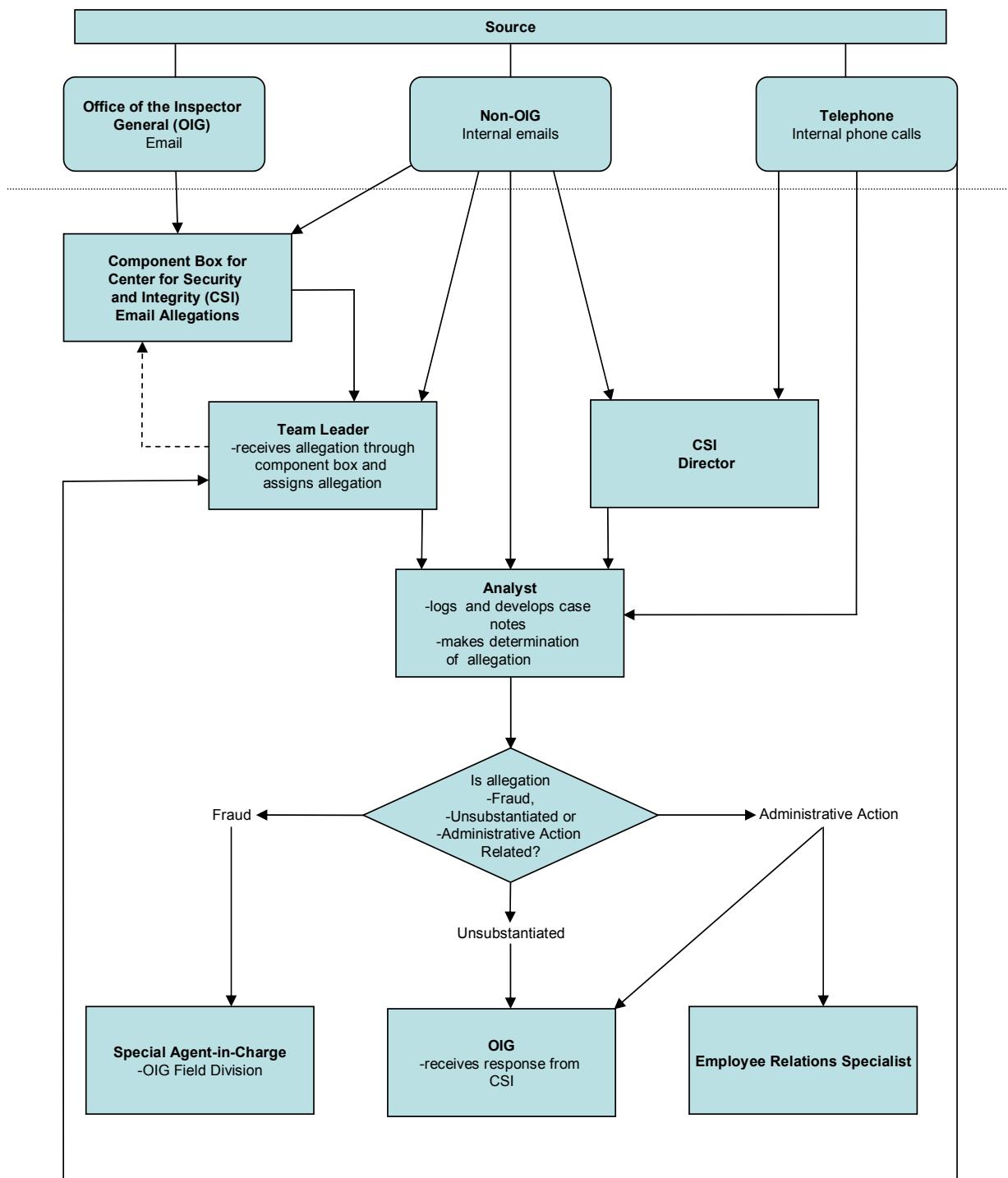
We performed field work at the SSA regional office in Dallas, Texas, and the OIG in Baltimore, Maryland, from April through August 2003. We determined that the computerized data used were sufficiently reliable to meet our audit objectives. The entity reviewed was the Dallas Regional Office under the Deputy Commissioner for Operations. We conducted our review in accordance with generally accepted government auditing standards.

Flowcharts

Allegation Referral Process Office of the Dallas Regional Commissioner



**CENTER FOR SECURITY AND INTEGRITY ALLEGATION REFERRAL
WORKFLOW
DALLAS REGIONAL OFFICE**



Appendix D

Employee Violations

LIST – EMPLOYEE POTENTIAL VIOLATIONS (Program Operations Manual System, GN 04112.005D)

Employee violations include but are not limited to situations in which an employee is suspected of willfully

- acting as an agent or attorney for prosecuting any Social Security claim before the Commissioner while an employee;
- disclosing without authorization any confidential information in violation of the Social Security Act or the Privacy Act of 1974;
- obtaining or attempting to obtain confidential information under false pretenses;
- making or causing to be made any false representation concerning the requirements of the Social Security Act or related provisions of the Internal Revenue Code;
- asking for, accepting, or agreeing to accept anything of value from a third party in return for executing or influencing the performance of official duties;
- participating in the planning or execution of any scheme or other activity under which a financial or other advantage improperly accrues or could accrue to any person or organization at the expense of the Government or parties with whom the Government may contract or otherwise deal;
- stealing or otherwise illegally disposing of refund remittances, Government checks, cash, directly deposited funds, or other obligations;
- illegally generating Social Security checks or depositing funds electronically to oneself or another;
- stealing or mutilating Government records, or destroying or removing them without authorization;
- violating conflict-of-interest laws as described in the Ethics in Government Act, the Standards of Ethical Conduct for Employees of the Executive Branch, and the SSA Guide on Employee Conduct;
- making or causing to be made any false statement or representation about wages, earnings, or self-employment income in connection with claims or the maintenance of earnings records;
- making or causing to be made any false statement or representation of a material fact in an application for payments or for a disability determination, or at any other time for use in determining rights to payments;
- concealing or failing to disclose a fact or event affecting initial or continued eligibility for payment;
- furnishing or causing to be furnished false information about identity in connection with a claim, issuing a Social Security number, or maintaining an earnings record;
- selling Social Security numbers/cards; or
- unlawfully disclosing, using, or compelling the disclosure of a Social Security number.

Appendix E

Social Security Administration Comments



SOCIAL SECURITY

MEMORANDUM

Date: February 5, 2004

To: Steven L. Schaeffer
Assistant Inspector General
For Audit

From: Horace L. Dickerson, Jr.
Regional Commissioner
Dallas

Subject: Dallas Region Reply: Employee Related Allegations (A-06-03-13075)

Thank you for the opportunity to review the OIG Audit of Employee-Related Allegations in Region VI (A-06-03-13075). We consider all employee allegations to be very serious. It is important that allegations are fully and promptly developed so that an employee can be cleared if the allegation is unsubstantiated or pursued criminally or administratively if substantiated.

We make every effort to ensure allegations with potential employee criminal violations are referred to the OIG and will continue to do so. In Dallas, we work closely with OIG OI and appreciate their support and assistance.

We appreciate your staff's review of the employee related allegation process in our Region and their recommendations which will help strengthen our controls and referral process. Our comments are attached. If members of your staff have questions, please have them call Carol Martinez at 214-767- 3585 in the Center for Security and Integrity, Management and Operations Support.

Attachments

RESULTS OF REVIEW AND RECOMMENDATIONS

The Dallas Region did not refer two potential criminal cases to the OIG for investigation.

This result related to two specific cases:

- One allegation involved an SSA employee who allegedly completed and signed claimants' signatures on low error profile redeterminations and cleared one overpayment waiver over \$2,000 without management approval. After receiving the finding, the Center Director (CD) for the Center for Security and Integrity (CSI) reviewed the CSI folder and the Center for Human Resources (CHR) folder. The CD recalled that the case had been discussed with the Special Agent in Charge prior to the referral to CHR. After a discussion of the facts, the decision was made to handle this case as a performance issue. However, documentation of this discussion was not in the file. A proposal to terminate was issued to the employee based on not following SSA policy and procedure. The employee failed to contact the claimants to obtain updated information to complete form SSA-8202. The claimants stated they did not sign the SSA-8202 nor did they give anyone permission to sign the form for them. The inaccurate information shown on the SSA-8202 appeared to have been obtained from aged information from other SSA sources. The employee elected to take early retirement rather than being terminated.

After receipt of the audit findings, CSI asked the Office of Investigation (OI) to review the allegation. OI replied that after reviewing they determined that the matter did not rise to a potential criminal issue for prosecutorial consideration by the U.S. Attorney's office. The OI also stated that this case had been discussed with the US Attorney during the OIG audit and the US Attorney had declined the case and stated that this matter should be handled administratively by the Agency. Training has been provided to the CSI staff to ensure that analysts are properly documenting cases prior to referral to the Employee and Labor Relations Specialist. In addition, the CSI analysts have been trained to officially refer cases with potential criminal violations to OI so that a written declination is part of CSI's file.

- The second case involved an employee discarding SSA records without authorization. CHR did not refer the case to OIG prior to taking administrative action. During the audit, OI informed the auditors that the allegation in question did not rise to the level that would merit a formal criminal investigation. Disciplinary action was taken to demote the employee to a lower grade. We concur with the finding that OI should have received the case for investigation before administrative action was taken, although OI agreed that the review revealed the action was appropriate. The CHR Team Leader took immediate action to inform the Employee and Labor Relations Specialists of this finding and provided a copy of POMS reference GN 04112.005 for future use.

There was inadequate case documentation to support whether allegations were properly resolved for 20 of 107 allegations.

- Four cases were referred by the Hot Line. In one case, two SSNs were involved. Although traffic documentation was in file, the analyst had not copied the ATS request and attached it to the ATS output. In this case, since there were no hits on the SSN the output was blank. Therefore, the absence of the ATS request made it appear as though traffic on the second SSN had not been requested. During the audit, we redeveloped the ATS request to show that the case had been accurately processed. We have now emphasized the need to always print the ATS request and attach it to the output. This requirement will also be added to CSI workflow procedures.
- The Dallas Region was unable to locate 16 case files. The 7-year retention refers to procedures for fraud allegations. The control log in CSI tracks all audit trail requests including those that are not employee related. The control log indicates that the unable to locate cases were not fraud allegations but systems violations (sanctions), no violation detected or non-employee cases. CSI refers substantiated systems violations (not criminal) directly to the employee relations staff in CHR. This staff maintains the official files related to administrative actions. Of the sixteen files, ten official files related to the systems violations were housed in CHR. Of the other six, the case control log showed that three cases involved non-employee audit trail requests and three involved systems violation allegations which were closed with no violations detected. We were unable to locate the six case files referred to above. We have improved our case control log to add a sequential numbering system, and the capability to sort based on type of case i.e., fraud, systems sanctions or both. This will assist our future reviews of employee-related cases. We will also review our workflow and address the retention period for audit trail requests involving unsubstantiated systems allegations (administrative). The CSI analysts have been trained to ensure that appropriate evidence which supports the clearance of employee-related allegations is maintained in the CSI folder.

The ORC did not retain control logs of allegations received.

The original ORC Action Item Flow Chart reviewed during the audit documented that employee related allegations are entered into the ORC Correspondence Control System, assigned a number and due date, entered into a paper action folder, and filed behind a due date. While an additional action also indicated that the item “is cleared” out of the Correspondence Control System and paper log, development documentation of the allegation remain housed on the electronic OPTIC control. This step was misleading in that the statement read “cleared out,” while the actual result is a “close out.”

We acknowledge that the wording in the flow chart should be revised to more accurately document how the control log is structured and maintained. We amended the flow chart to document this clarification and have also begun the development of a locally controlled electronic file.

The ORC's Intranet database did not have adequate safeguards to prevent unauthorized access to employee allegations.

We agree that our current Intranet database does not adequately restrict unauthorized access to employee allegations. The limited user access instituted—highly restricted instruction and knowledge of web address--reduced the likelihood that unauthorized usage would occur. However, we agree that additional safeguards are necessary to limit access. We are designing a new electronic control file that will restrict access by authorized employee name, position, and PIN. In the meantime, we are applying security measures to our existing control system that will restrict use, based on the user's authority to access the records.

Retention of Control Logs

The ORC did not have a complete list of allegations received from October 1, 2000 through March 27, 2002.

The allegations received from October 1, 2000 – March 27, 2002 were closed out on the electronic control file but paper files of completed case documentation were retained. The Region maintains hard copies of files for two years, per SSA policy. An electronic version of the allegations is also readily available, but per the response above, the electronic controls will have to be upgraded with additional security assurances. We are designing a new electronic control file that will augment the hard copy documentation.

CSI did not have an adequate allegation tracking system.

There were two findings in this area:

- The database did not have a sequential control number. This has been fixed. We now have a sequential control number.
- In one case, an allegation was received from the Hot Line but did not appear on the control log. Allegations from the Hot Line come to the component email box and will now be logged in and assigned by the Team Leader or Center Director.

Appendix F

OIG Contacts and Staff Acknowledgments

OIG Contacts

Paul Davila, Director, (214) 767-6317

Acknowledgments

In addition to those named above:

Lela Cartwright, Auditor-in-Charge

Wanda Renteria, Auditor

Kimberly Beauchamp, Writer-Editor

For additional copies of this report, please visit our web site at <http://www.ssa.gov/oig> or contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-1375. Refer to Common Identification Number A-06-03-13075.

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, Subcommittee on Human Resources
Chairman and Ranking Minority Member, Committee on Budget, House of Representatives
Chairman and Ranking Minority Member, Committee on Government Reform and Oversight
Chairman and Ranking Minority Member, Committee on Governmental Affairs
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 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

Office of Audit

The Office of Audit (OA) conducts comprehensive financial and performance audits of the Social Security Administration's (SSA) programs and makes recommendations to ensure that program objectives are achieved effectively and efficiently. Financial audits, required by the Chief Financial Officers' Act of 1990, assess whether SSA's financial statements fairly present the Agency's financial position, results of operations and cash flow. Performance audits review the economy, efficiency and effectiveness of SSA's programs. OA also conducts short-term management and program evaluations focused on issues of concern to SSA, Congress and the general public. Evaluations often focus on identifying and recommending ways to prevent and minimize program fraud and inefficiency, rather than detecting problems after they occur.

Office of Executive Operations

The Office of Executive Operations (OEO) supports the Office of the Inspector General (OIG) by providing information resource management; systems security; and the coordination of budget, procurement, telecommunications, facilities and equipment, and human resources. In addition, this office is the focal point for the OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act. OEO is also responsible for performing internal reviews to ensure that OIG offices nationwide hold themselves to the same rigorous standards that we expect from SSA, as well as conducting investigations of OIG employees, when necessary. Finally, OEO administers OIG's public affairs, media, and interagency activities, coordinates responses to Congressional requests for information, and also communicates OIG's planned and current activities and their results to the Commissioner and Congress.

Office of Investigations

The Office of Investigations (OI) conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement of SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, physicians, interpreters, representative payees, third parties, and by SSA employees in the performance of their duties. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Counsel to the Inspector General

The Counsel to the Inspector General provides legal advice and counsel to the Inspector General on various matters, including: 1) statutes, regulations, legislation, and policy directives governing the administration of SSA's programs; 2) investigative procedures and techniques; and 3) legal implications and conclusions to be drawn from audit and investigative material produced by the OIG. The Counsel's office also administers the civil monetary penalty program.