OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

FOLLOW-UP ON THE SOCIAL SECURITY ADMINISTRATION'S MONITORING OF POTENTIAL EMPLOYEE SYSTEMS SECURITY VIOLATIONS

October 2007 **A-14-07-17102**

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: October 29, 2007 Refer To:

To: The Commissioner

From: Inspector General

Subject: Follow-up on the Social Security Administration's Monitoring of Potential Employee Systems Security Violations (A-14-07-17102)

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) implemented recommendations made in our July 2004 report, *The Social Security Administration's Monitoring of Potential Employee Systems Security Violations* (A-14-04-23004).

BACKGROUND

In June 1998, SSA established a uniform set of *Sanctions for Unauthorized Systems Access Violations*[1] (Sanctions) to secure the integrity and privacy of the personal information contained in the Agency's computer systems and to ensure that any violations of the confidentiality of its computer records are treated consistently. For more information on Sanctions see Appendix B.

In the document, *Rules of Behavior for Users and Managers of SSA's Automated Information Resources*,[2] the Agency describes what behavior is expected of all SSA personnel, contractors, and external users of SSA's automated information systems resources.

Managers are the primary lines of defense against employee systems security violations. SSA's Integrity Review Handbook outlines the procedures for managers to use when conducting integrity reviews.[3] In an effort to prevent and uncover potential

---

[1] Information Systems Security Handbook (ISSH), Chapter 4 References, Office of Labor Management and Employee Relations website, *Sanctions for Unauthorized System Access Violations, Attachment: Commissioner's Memorandum*, June 22, 1998.

[2] *Rules of Behavior for Users and Managers of SSA's Automated Information Resources,* http://eis.ba.ssa.gov/ssasso/issh/rulesofbehavior.htm.

[3] Integrity Review Handbook, Chapter 1, April 4, 2006.

employee systems security violations, SSA developed the Comprehensive Integrity Review Process (CIRP), a monitoring tool to detect specific SSA mainframe systems activity that is considered potential fraud or misuse by employees. CIRP uses predetermined criteria to identify certain queries input by employees and generates reports for management review. SSA has developed a schedule of administrative sanctions or penalties to address people who have inappropriately used SSA's systems and information. For additional background information, see Appendix B and for our scope and methodology, see Appendix C.

The Office of Management and Budget (OMB) guidance[4] states:

> …safeguarding personally identifiable information[5] (PII) in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974.

RESULTS OF REVIEW

We determined that SSA has implemented our recommendations. At the time of our original audit, we noted problems with classifying violations with the correct severity level, maintaining sufficient documentation and providing appropriate case documentation to the Office of the Inspector General (OIG) in a timely manner. SSA has improved in these areas and is working to ensure that these issues are dealt with sufficiently and appropriately.

We found during our current review that the Agency could improve the system security violation monitoring and reporting process by incorporating the following suggestions:

- Periodically issue electronic or written reminders concerning the retention of supporting documentation for systems security violations according to SSA's policy;

- Implement a pilot where the OIG is provided all employee potential misuse and potential fraud systems security violations for two headquarters components and one regional office for 6 months;

---

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

[5] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- Provide OIG with all potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation, to assess the information for potential criminal activity; and

- Evaluate and modify policies and procedures to ensure employee violations of Automated Information Resources Rules of Behavior are appropriately addressed.

Recommendations from Our Prior Review

Recommendation 1: We recommended SSA establish policies and procedures on retaining all supporting documentation for potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation, so that resolutions are accessible and verifiable.

The Agency agreed with our recommendation and stated that their current policy and procedures require reasonable retention of documentation necessary to ensure effective resolution of and consistent application of Sanctions for such cases. SSA agreed to issue reminders to management concerning these policies and procedures to assure that adequate documentation is maintained.

We reviewed SSA's current policies and procedures, Operational and Administrative Records Schedules (OARS) on retaining all supporting documentation for potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation. We determined the Agency's retention policy and procedures appear appropriate to address the Agency's need in this area.

Recommendation 2: We recommended SSA maintain supporting documentation for all potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation, to ensure appropriate and consistent Sanctions are applied within the Agency.

The Agency agreed with recommendation 2 and indicated they would send out reminders as needed for management to maintain supporting documentation. During our review of 108 cases, we observed that SSA has improved on its retention of documentation related to potential systems security violations since the original audit. According to SSA, oral reminders were periodically issued to staff. As SSA experiences significant human capital turnover, we encourage SSA to ensure the integrity of the security violations review process and consider periodically issuing electronic or written reminders to managers to maintain all documentation associated with systems security violations for 4 years as required by SSA policy.

Recommendation 3: We recommended SSA provide OIG with periodic access to the potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation, to assess the information for potential criminal activity.

The Agency agreed with this recommendation. In response to recommendation 3, SSA provided OIG access to 6 months, January 2004 to June 2004, of data for cases where administrative action had already occurred. The Office of Operations evaluated the referral process and determined it would continue to refer only cases to OIG that the Agency determined were Category III cases. At that time, the OIG was enhancing its investigative database and revised the electronic 8551 (e-8551) fraud reporting form. OIG was expanding the use of the e-8551 on SSA Intranet sites to alert managers to the new process and encourage them to use it. These actions were completed after the pilot in 2004. Since an automated process exists, it would be beneficial to perform a new pilot. Our suggestion is that all potential misuse and potential fraud system security violations for two headquarters components and one regional office be submitted to the OIG for a 6-month period. Appendix E details the number of staff per SSA Office, related transactions, and reported violations. During the pilot period, SSA could assess the effectiveness and consistency of monitoring and processing system security violations Agency-wide.

Our review of the 108 cases showed that the Agency has improved on its categorization of the systems security violation cases. During our original audit, we observed numerous instances where violations that should have been Category IIB or III were categorized as a Category I or IIA. We did not find any instances of that problem during the current review.

As mandated by the Inspector General Act of 1978, the OIG is responsible for preventing and detecting fraud and abuse in agency programs and operations.[6] The Office of Investigations within the OIG, protects the integrity of SSA's programs by investigating allegations of fraud, waste, and abuse.[7] For this reason, such cases should be referred to the OIG early in the administrative sanction development process to ensure fulfillment of the OIG's responsibilities and the effective enforcement of SSA's and OIG's mission.

We found that 3 of the 108 administratively sanctioned cases were referred to the OIG by SSA. Specifically, the Agency referred two Category III cases and a Category IIB case to OIG. In addition, one Category IIB and one Category III violation case were referred to the OIG by outside sources. The Category IIB case was referred to OIG by a local law enforcement agency. In this case, the employee improperly accessed

[6] 5 U.S.C. App. 3, Section 2.

[7] OIG Manual System, OI Special Agent Handbook, Chapter 1, Section 001.020, p. 1-3.

SSA's Systems and disclosed the information to an unauthorized individual. With the recent release of OMB Memorandum M-07-16,[8] in the future an SSA manager should send the case to OIG to review since this would be considered a breach of PII. The OMB guidance states safeguarding PII and preventing its breach is the responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, agencies' Inspectors General and other law enforcement, and public and legislative affairs.[9] The second case was referred to the OIG by an anonymous caller to the Hotline.[10] This Category III case entailed an employee who was using SSA's System to maintain or support a personal business. According to the Agency's Rules of Behavior,[11] SSA prohibits the use of e-mail to maintain or support a personal business. This case may not have been referred by SSA because the Agency is not recognizing and applying the same Systems Security Violation Sanctions to the improper computer use cases.

During our audit of SSA's Incident Response and Reporting System,[12] we identified other instances of improper computer use or improper use of PII that were detected outside of the CIRP process. For example, we identified cases of computer misuse involving an SSA employee and a Disability Determination Service (DDS) employee. In one case, an SSA employee had unauthorized password cracking software on an SSA workstation. An employee could use password cracking software repeatedly to try to guess users' passwords to gain unauthorized access to a system, and to retrieve all the files on an individual's computer, or even log in to a computer. The employee was told to remove the software from his computer, but no administrative action was taken against him. In another case, a DDS employee e-mailed 55 claimants' SSNs, names, and case numbers to a "Hotmail" e-mail account. The employee sent 3 e-mails containing PII on the 55 claimants outside of SSA's secure network. This employee just returned from a 10-day suspension for a separate unrelated disciplinary action. Only one of these two cases was referred to the OIG and this case was referred after we informed the Agency of our findings. It appears that SSA is not recognizing and applying the same Systems Security Violation Sanctions to these improper computer use cases. All computer-related and PII cases that violate the Agency's Rules of

---

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

[9] Id.

[10] The SSA OIG Fraud Hotline provides an avenue for individuals to report fraud, waste, and abuse within the SSA's programs and operations. The Hotline handles allegations regarding violations of law or regulations affecting SSA programs and operations.

[11] *Rules of Behavior for Users and Managers of SSA's Automated Information Resources,* http://eis.ba.ssa.gov/ssasso/issh/rulesofbehavior.htm.

[12] OIG Final Report, *The Social Security Administration's Incident Response and Reporting System*, A-14-07-17070, dated August 3, 2007.

Behavior[13] need to have appropriate Sanctions applied. Where potential fraud or possible criminal activity is involved, cases should be forwarded to the OIG. SSA needs to modify policies and procedures that ensure employee systems security violations of Automated Information Resources Rules of Behavior are appropriately addressed.

As noted in the background section, protecting PII is a highly significant issue for the Federal Government. The importance of protecting PII is emphasized by the recent guidance and requirements in this area issued by OMB. Based on the increased emphasis placed on protecting PII, OIG believes that some level of investigation by our office is warranted for those cases designated by SSA managers as potential misuse or potential fraud systems security violations. This investigation should occur prior to applying administrative actions.

We would like to encourage the Agency to send all category III violations and cases that managers determine need further investigation to the OIG. In addition, the Agency should remind managers that systems security violations are not limited to the CIRP process as previously described but may include other breaches of PII such as sending PII home through e-mail. Finally, SSA should send any appropriate cases found outside of CIRP to the OIG.

Recommendation 4: We recommended that SSA continue to ensure all integrity reviews are conducted in a more timely and in-depth manner.

The Agency agreed with this recommendation and stated they already devote significant resources to monitor accurate and timely completion of CIRP alerts.

During our review of the 108 administratively sanctioned cases, we estimated 85 percent of the sanctions were applied within 1 year of the violation (see the Table below). We appreciate SSA's efforts to adequately address our recommendation to perform these reviews in a more timely and in-depth manner. We encourage the Agency to continue to expedite the review process to minimize the number of cases that take longer than 1 year to process. This will ensure the Agency's ability to protect the integrity and privacy of the personal information contained in its computer systems.

[13] *Rules of Behavior for Users and Managers of SSA's Automated Information Resources,* http://eis.ba.ssa.gov/ssasso/issh/rulesofbehavior.htm.

Administrative Sanction Processing Times	Number of Cases Reviewed	Percentage of Cases Reviewed
Less than or equal to 12 months-see note	92	85.2
Greater than 1 year and less than 3 years	8	7.4
Over 3 years	8	7.4
TOTAL	**108**	**100**

Note-This includes 4 cases where employees resigned or their resignation was pending.

CONCLUSION AND RECOMMENDATIONS

SSA has made progress in addressing the four recommendations of our prior audit. SSA has established policies and procedures to retain and maintain the systems security violations documentation. In addition, the Agency is performing the integrity reviews more timely and in an in-depth manner. We encourage the Agency to continue its efforts to implement corrective actions to improve its systems security violation review process. However, to strengthen SSA's integrity review process and reduce its vulnerability to employee systems security violations, we recommend SSA:

1. Continue to send electronic or written reminders concerning retention of supporting documentation for systems security violations according to SSA's policy.

2. Implement a pilot where the OIG is provided all employee potential misuse and potential fraud systems security violations for two headquarters components and one regional office for 6 months.

3. Provide OIG with all potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation, to assess the information for potential criminal activity.

4. Evaluate and modify procedures to ensure all employee violations of Automated Information Resources Rules of Behavior are appropriately detected, reported, documented, and resolved across the organization.

AGENCY COMMENTS

SSA generally agreed with all our recommendations. See Appendix F for the full text of SSA's comments.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

ATS	Audit Trail System
CIRP	Comprehensive Integrity Review Process
DDS	Disability Determination Service
DSSPI	Division of Systems Security and Program Integrity
FISMA	Federal Information Security Act of 2002
FY	Fiscal Year
ISSH	Information Systems Security Handbook
OARS	Operational and Administrative Records Schedule
ODAR	Office Disability Adjudication and Review
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPSOS	Office of Public Service and Operations Support
PII	Personally Identifiable Information
Sanctions	Sanctions for Unauthorized Systems Access Violations
SSA	Social Security Administration

Background

This is a follow-up of our July 2004 report, *The Social Security Administration's Monitoring of Potential Employee Systems Security Violations* (A-14-04-23004). In the Comprehensive Integrity Review Process (CIRP), the manager determines whether queries are considered: 1) No Problem; 2) Potential Violation - Misuse; 3) Potential Violation - Fraud; or 4) Not-Certified – Investigation Pending. CIRP reviews must be completed and certified in a certain period of time depending on the type of review. For example, CIRP query reviews need to be completed and certified by the end of each month. If a potential security violation (misuse or fraud) is identified, the appropriate security staff[1] must be contacted to advise managers on the appropriate action to be taken. While the information in the CIRP query system is retained for a short period of time, the history of employees is maintained in the Audit Trail System (ATS) for 7 years. The ATS is designed to provide SSA security officers with the capability to monitor SSA data entry activities nationwide.

Annually, all employees are required to read and sign the *Acknowledgment Statement* indicating that they have read and understand the sanctions.[2] The Sanctions and *Acknowledgment Statement* have both been incorporated into the Information Systems Security Handbook. Employees who violate the established rules are subject to the Agency's Sanctions for systems misuse as follows:

Systems Security Violation Category and Sanction

Category	First Time Offense	Sanction
I	Unauthorized access without disclosure	2-day suspension
IIA	Disclosure of information to an individual entitled to the information	2-day suspension
IIB	Disclosure of information to an individual not entitled to the information	14-day suspension
III	Unauthorized access for personal gain or with malicious intent	Removal

[1] Integrity Review Handbook, Release 3, Chapter 1, Query Review, p. 4, August 2003.

[2] Information Systems Security Handbook, Chapter 4 References, Office of Labor Management and Employee Relations website, *Sanctions for Unauthorized System Access Violations, Attachment: Commissioner's Memorandum*, June 22, 1998.

Scope and Methodology

Our scope was limited to a determination of whether the Social Security Administration (SSA) has taken sufficient measures to implement the recommendations in our 2004 report. We reviewed 108 cases from 5 regional offices,[1] the Office of Central Operations and the Office of Disability Adjudication and Review for Fiscal Year (FY) 2006. For each case, we examined the Standard Form 50, Notification of Personnel Action, and the adverse action documentation to determine whether the Agency consistently applied its Sanction policy in a timely manner. We compared all 108 cases to the National Investigative Case Management System to determine if all cases were referred to the Office of the Inspector General for investigation. We also confirmed the total number of administratively sanctioned cases provided from the Office of Public Service and Operations Support (OPSOS) with the cases received from each of the offices. In addition, we also:

1. Reviewed the following criteria:

   - Federal Information Security Management Act of 2002 (FISMA);[2]
   - Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources;*
   - OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007;
   - SSA's Operational and Administrative Records Schedule's guidance on personnel records;
   - SSA's Information Systems Security Handbook;
   - SSA's *Rules of Behavior for Users and Managers of SSA's Automated Information Resources;*
   - SSA's Program Operations Manual System; and
   - SSA's Integrity Review Handbook.

[1] The same five regions as the original audit, New York, Philadelphia, Atlanta, Dallas, and San Francisco.

[2] P.L. No. 107-347, Title III, section 301, codified at 44 U.S.C. § 3541 (1).

2. Interviewed representatives from SSA's:

   - Office of Operations, OPSOS, and Division of Systems Security and Program Integrity (DSSPI). DSSPI monitors integrity reviews in the regions and the processing centers to ensure the reviews are performed timely and consistently;
   - Office of Systems Security Operations Management, which has national oversight of the integrity review process;

We performed our field work at SSA Headquarters between December 2006 and May 2007. We determined that the data used in this report was sufficiently reliable to meet our audit objectives and intended use of the data. We determined that our use of this data should not lead to an incorrect or unintentional message. We conducted our review in accordance with generally accepted government auditing standards.

Sanction Cases Reviewed for Fiscal Year 2006 Systems Security Violations

Social Security Administration Region\ Offices	Cases OIG Received				
	Offenses				
	Cat. I	Cat. IIA	Cat. IIB	Cat. III	Total
5 Regions					
New York	14	2	6	0	22
Philadelphia	13	9	1	0	23
Atlanta	19	5	2	1	27
Dallas	8	1	0	1	10
San Francisco	13	3	1	0	17
Headquarters					
Office of Central Operations	4	0	1	0	5
Office of Disability Adjudication and Review	2	0	1	1	4
Total	**73**	**20**	**12**	**3**	**108**

Comparison of Systems Access, Transactions, and Security Violations for Fiscal Year 2006

Social Security Administration Offices	Number of Employees with Systems Access	Number of Query CIRP Transactions*	Number of Systems Security Violations
Office Of Operations	65,159	12,984,139	128
Office of Systems	8,334	4,196	0
Office of Disability Adjudication and Review	7,876	14,831	4
Office of Quality	1,306	113,395	0
Office of Budget Finance and Management	963	1,467	0
Office of Disability and Income Security Programs	837	9,896	0
Office of the Inspector	621	312,418	0
Office of General Counsel	571	2,967	0
Center for Medicare and Medicaid Services	505	1,358	0
Office Human Resources	412	3,157	0
Office of Communications	177	11,910	0
Office of Policy	128	192	0
Office of Legislation and	53	314	0
Office of Actuary	53	1,667	0

*CIRP – Comprehensive Integrity Review Process.

This chart shows that the Office of Operations is reporting the majority of violations and also has the most staff with the most mainframe access. The Office of Disability Adjudication and Review was the only other office that reported system security violations.

Agency Comments

MEMORANDUM

Date: October 4, 2007 Refer To: S1J-3

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

From: Larry W. Dye /s/

Subject: Office of the Inspector General (OIG) Recommendation Reconsideration Letter, "Follow-up on the Social Security Administration's Monitoring of Potential Employee Systems Security Violations" (A-14-07-17102)—INFORMATION

In response to your September 12, 2007 request to reconsider our response to recommendation 4, we now agree based on the revised language you provided for that recommendation. The attached response to recommendation 4 now reflects that we agree, while the response to recommendations 1 through 3 remains unchanged.

Please let me know if we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "FOLLOW-UP ON THE SOCIAL SECURITY ADMINISTRATION'S MONITORING OF POTENTIAL EMPLOYEE SYSTEMS SECURITY VIOLATIONS " (A-14-07-17102)

Thank you for the opportunity to review and comment on the draft report. We appreciate your conducting this follow-up audit of the Social Security Administration's (SSA) monitoring of potential employee systems security violations. Our responses to the specific recommendations are provided below.

Recommendation 1

Continue to send electronic or written reminders concerning retention of supporting documentation for systems security violations according to SSA's policy.

Comment

We agree. We have provided reminders in the past and will continue to send written and electronic reminders to management about the need to retain supporting documentation regarding systems security violations. In September 2007, we issued a reminder to managers to retain supporting documentation for systems security violations development.

Recommendation 2

Implement a pilot where OIG is provided all employee potential misuse and potential fraud systems security violations for two headquarters components and one regional office for 6 months.

Comment

We partially agree. We still do not believe there is any value in providing information on cases of misuse in which fraud is not involved. We will, however, work with OIG to develop a process to submit information on all potential misuse cases for one region and two headquarters components for a six month period.

Recommendation 3

Provide OIG with all potential misuse or potential fraud employee systems security violations, as identified by SSA managers as needing further investigation, to assess the information for potential criminal activity.

Comment

We partially agree. As in the past, we will continue to refer all Category III violations to OIG via the electronic 8551 fraud reporting form. We will continue to refer other category violations where fraud or possible criminal activity exists. This includes violations discovered through the

Comprehensive Integrity Review Process. As stated in our response to recommendation 2, we do not see value in referring all potential violations to OIG as the vast majority of these do not involve fraud, criminal intent or criminal activity.

Recommendation 4

Evaluate and modify procedures to ensure all employee violations of the Automated Information Resources Rules of Behavior are appropriately detected, reported, documented and resolved across the organization.

Comment

We agree. We already have policies in place to address violations. Our records show that when we detect violations, we have taken the appropriate disciplinary measures, documented our actions and reported the violations to OIG when warranted. We investigate violations and potential misuse, and if fraud is suspected, we refer the cases to OIG. Sanctions for Unauthorized Systems Access Violations (Sanctions) policies are applied when appropriate. However, not all failures to comply with the Rules of Behavior fall under Sanctions policies and when appropriate progressive discipline is applied instead of the sanction policies. We believe progressive discipline is the appropriate manner to address the types of activities provided as examples in the audit report and do not believe that they should be included in the systems Sanctions policy. Penalties under progressive discipline may be as severe as penalties imposed under Sanctions policies.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Data Analysis and Technical Audit Division, (410) 965-9702

Phil Rogofsky, Audit Manager, Network Security and Telecommunications Branch, (410) 965-9719

Acknowledgments

In addition to those named above:

Mary Ellen Moyer, Senior Program Analyst

Deborah Kinsey, 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 Specialist at (410) 965-3218. Refer to Common Identification Number A-14-07-17102.

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

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises 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 and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity 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 OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG 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. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.