OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S MONITORING OF POTENTIAL EMPLOYEE SYSTEMS SECURITY VIOLATIONS

July 2004 A-14-04-23004

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: July 27, 2004 Refer To:

To: The Commissioner

From: Acting Inspector General

Subject: The Social Security Administration's Monitoring of Potential Employee Systems Security Violations (A-14-04-23004)

OBJECTIVE

Our objectives were to examine the processes that the Social Security Administration (SSA) has in place to review potential employee systems security violations in a timely and proper manner and to limit SSA's exposure to employee misuse of its systems. We also examined the process used to refer violations to the Office of the Inspector General (OIG).

BACKGROUND

In April 2003, we issued an early alert memorandum[1] in response to the Commissioner's concerns as to whether SSA had a process in place to ensure that all potential employee systems security violations were resolved in a timely, comprehensive, and consistent manner. We reported that there were limited controls in place to ensure that potential employee systems security violation and fraud cases were appropriately monitored, reviewed and reported in accordance with SSA's policy. We initiated this review as part of the OIG's efforts to assist SSA in improving its security and integrity review process.

SSA stated in a March 2000 memorandum[2] that in June 1998, it established a uniform set of *Sanctions for Unauthorized Systems Access Violations* (Sanctions) to secure the integrity and privacy of 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. This memorandum advised SSA employees of the categories

[1] OIG Memorandum, *Early Alert: The System Security and Integrity Review Process*, A-14-04-24003, April 11, 2003.

[2] Memorandum, *Revisions to Sanctions for Unauthorized Systems Access Violations—INFORMATION*, March 2, 2002, (as of September 10, 2003).

of systems security violations and the minimum recommended sanctions. Table 1 below shows those sanctions for first time offenses. Those sanctions apply for all SSA employees who use or have access to computer systems containing personal data about workers, claimants, beneficiaries, SSA employees or other individuals.

Table 1. 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

Annually, all employees are required to read and sign the *Acknowledgment Statement* indicating that they have read and understand the sanctions.[3] The Sanctions and *Acknowledgment Statement* have both been incorporated into the Information Systems Security Handbook. For additional background information, see Appendix B and for our scope and methodology, see Appendix C.

RESULTS OF REVIEW

We found that SSA has a process in place to review potential employee systems security violations and has taken steps to limit its exposure to employee misuse of its systems.[4] These steps include, but are not limited to:

- Establishment of the Sanction Penalties;
- Establishment of policies and procedures for reviewing potential employee systems security violations in the Information Systems Security Handbook[5] and the Integrity Review Handbook[6] (the Handbook);
- Development of the Comprehensive Integrity Review Process (CIRP) system to alert managers of potential problems;
- Efforts to analyze trends in applying sanctions;

[3] Information Systems Security Handbook, Chapter 21, *Sanctions for Unauthorized System Access Violations, Attachment: Commissioner's Memorandum*, June 22, 1998.
[4] Potential employee systems security violations are defined through out this report as an instance where an SSA Manager designates that an employee has committed a potential misuse or potential fraud and indicates that further review is required to determine if an administrative action is appropriate.
[5] Ibid.
[6] Integrity Review Handbook, Release 3, August 2003.

- Efforts to work with OIG to refer cases to the OIG; and
- Periodic training and reminders for the reviewers.

We requested employee systems security sanction cases from all components. Only the Office of Operations (Operations) provided sanction cases for our review. While it is true that Operations has the majority of employees with access to SSA's systems, it would seem unlikely that no employee in any other component has committed a systems security violation since September 2000.

While we believe that the Agency, and in particular Operations, is making a concerted effort to address employee systems security violations, there are areas within the integrity review process that need improvement.

CERTAIN POTENTIAL SECURITY VIOLATION CASES WERE NOT REFERRED TO THE OIG

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.[7] The Office of Investigations (OI), within the OIG, protects the integrity of SSA's programs by investigating allegations of fraud, waste, and abuse.[8] 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 and OIG mission.

We reviewed 308 administratively sanctioned cases at 5 regional offices between September 2000 and August 2003. One of the purposes for this review was to determine how many of these cases should have been referred to the OIG. It is our opinion that any unauthorized access of SSA's systems and data must be considered potential fraud until an analysis by OIG personnel determines otherwise. SSA administrative sanctions are in addition to any criminal penalties prescribed by law.

We found that SSA, and particularly Operations, has a process in place to review potential employee systems security violations. Although Operations has taken steps to limit its exposure to employee misuse of its systems, we determined that all 308 cases should have been referred to the OIG for investigation. We found that only 26 of the 308 administratively sanctioned cases were referred to the OIG. Of the 26 cases, 17 were referred to us by the Agency. The remaining nine cases were referred to us by outside sources. One of the five regions we reviewed did not refer any cases. Although SSA's Program Operations Manual System provides criteria and procedures for referring fraud cases to the OIG, we noted that the Handbook that is used to perform integrity reviews does not clearly specify these criteria or procedures. We believe this lack of clarity contributes to the low number of cases referred to OIG.
Some examples of sanctioned cases that should have been referred are:

[7] 5 U.S.C. App. 3, Section 2.
[8] OIG Manual System, *OI Special Agent Handbook*, Chapter 1, Section 001.020, pages 1-2.

- An employee improperly accessed over 1,400 records over a 2-month period. This employee committed a Category III violation and was removed from service.

- An employee accessed the records of clients for their outside tax business. This unauthorized access occurred for 2 years before it was discovered. This employee committed a Category III violation and, as stated in SSA policy,[9] should have been removed from service; however, the employee resigned upon reaching a settlement agreement with the Agency.

- An employee committed a Category I violation and received a 3-day suspension. After the suspension, SSA management was advised by a friend of the employee on two separate occasions that the employee was suspected of accessing the friend's personal information. No action was taken by SSA for these allegations. Local law enforcement attempted to arrest the employee at SSA for a domestic dispute involving the friend. SSA informed the OIG of the attempted arrest and the OIG assisted the local law enforcement with the employee's arrest 5 days later. The arrest for the domestic dispute led to an investigation of systems security violations by SSA and the employee was given a 15-day Category IIA suspension. SSA did not refer the systems security violation case to the OIG.

The Agency is working with OIG on the case referral procedure. Currently, the Agency does not refer Category I or II sanction cases unless, in its opinion, potential criminal activity has occurred. However, the OIG believes that, prior to applying administrative actions, 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.

We believe that failure to refer cases designated by SSA managers as potential systems security violations for further investigation to OIG undermines the Agency's ability to deal appropriately with fraud and abuse. As a result, individuals who committed serious violations may have escaped our investigation and avoided removal and/or prosecution. Some of these individuals may continue to work for SSA, and remain in a position that enables additional systems abuses. Several employees, who committed potentially criminal offenses, were allowed to retire or resign before sanctions could be applied. These individuals may have been liable for criminal or civil penalties if an investigation had been conducted. As a result, the employees may be rehired by the Agency since there is no permanent record showing the prior systems security violations; however, criminal and civil prosecution could avoid this outcome. Additionally, criminal and civil penalties could be used to provide a strong deterrent to

[9] Information Systems Security Handbook, Chapter 21, *Sanctions for Unauthorized System Access Violations*, Attachment: Deputy Commissioner for Human Resources Memorandum, page 4, March 2, 2000.

future potential systems security violations.

CERTAIN VIOLATIONS WERE NOT ADDRESSED TIMELY IN CONFORMANCE WITH THE INTEGRITY REVIEW PROCESS

The Handbook requires managers to conduct reviews on a daily, weekly or monthly basis depending on the type of review. The CIRP system generates various reports to assist and facilitate managers in performing timely reviews. Additionally, Operations recently provided managers with CIRP training on the integrity review process. While the Agency is working diligently to address employee systems security violations, we found cases where an employee's inappropriate activities were not discovered for an extended period of time. These cases suggest that the CIRP reviews need to be conducted in a more timely and in-depth manner.

For example:

- An employee performed 50 unauthorized queries for more than 3 years and disclosed personal information to a co-worker who was committing credit card fraud. When his activity was discovered, this employee was given a 14-day suspension, which is a Category IIB sanction for a first-time access and disclosure offense.

- An employee performed 230 unauthorized queries of the records of friends for more than 3 years and disclosed some of this information to individuals not entitled to the information. This activity was punished as a first-time offense, and the employee was given a 10-workday suspension.

- An employee performed unauthorized queries on relatives over a 4-year period. Upon discovery of this activity, the employee was given a 2-day suspension, which is the sanction for a first-time Category I violation.

Based on documentation currently available, we were not able to determine why these activities went on so long before they were addressed. If CIRP reviews are not performed timely and adequately, employees' unauthorized use of the systems may continue undetected and will undermine the Agency's efforts to protect the integrity and privacy of the personal information contained in its computer systems.

NO CENTRALIZED SYSTEM OR PROCESS EXISTS TO TRACK EMPLOYEE SYSTEMS SECURITY VIOLATIONS

Office of Management and Budget (OMB) Circular A-123*, Management Accountability and Control,* states "…management controls are the organization, policies, and procedures used to reasonably ensure that programs and resources are protected from waste, fraud, and mismanagement."[10] SSA does not have an agency-wide centralized system or process to track employee systems security violations. Operations does compile a cumulative report of all systems security violations since the Sanctions policy was initiated in 1998. This report, however, does not include detailed information such as the names or Social Security numbers of the individuals sanctioned. The report is a summary of reports provided by the different regional offices and the Operations components at Headquarters, and is used to analyze the systems violation sanction process. To verify the numbers in the report requires accessing the individual sanctioned case folders maintained at the 10 regional offices and Headquarters. However, based on the information provided at each region, we were still unable to reconcile the cumulative report to the listings of systems security violation cases provided by the regional offices because of the lack of detailed information maintained in the report.

For a centralized system to be effective, it should flow from first line managers to their local security staff to a headquarters component, such as the Chief Security Officer within the Office of the Chief Information Officer. According to the Agency's integrity review requirements, the appropriate security staff should be contacted for assistance after the reviewer determines that a potential violation exists.[11] We found the managers did not always contact the appropriate security staff upon discovery of potential security violations. As a result, the reviewers are not always appropriately counseled in determining whether further action is necessary or whether the cases should be sent to OIG.

Because a centralized system does not exist, managers cannot be certain whether an employee has committed any prior systems security violations. Therefore, penalties for repeat offenders may not be applied appropriately, particularly if the employee has changed offices or regions. Additionally, it is difficult to properly safeguard the information entrusted to the Agency without a centralized system. Furthermore, all potential systems security violations should be input into such a system so they can be tracked from discovery to resolution.

We believe the Agency's security staff should receive all potential violation cases from the managers. In addition, SSA should develop an agency-wide centralized system or process with the potential violation information included by the appropriate security staff. SSA could consider expanding the current reporting process used by Operations to the entire Agency and ensure that all necessary information is included.

[10] OMB Circular A-123, *Management Accountability and Control,* Section 2. Policy, as revised page 1, June 21, 1995.

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

SANCTION DOCUMENTATION WAS NOT LOCATED FOR ALL CASES

According to OMB, "...systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability."[12] An effective integrity review system requires that adequate documentation be maintained.

We requested all 308 Official Personnel Folders (OPF) from SSA and received documentation as follows:

- 245 had the appropriate documentation;
- 24 did not contain SF-50 forms corresponding to the imposed sanctions as required by Office of Personnel Management policy;[13]
- 22 were not located for employees who were separated from service. These folders had been sent to the National Personnel Records Center in St. Louis, Missouri, 30 days after the employees separated from Federal service; and
- 17 were not located.

SF-50s were not provided for 63 of the 308 cases reviewed. These forms are placed in the OPF as a permanent record of actions for promotion, reassignment, suspension, and return to duty. Without this documentation, SSA has no permanent record showing that these employees had been previously sanctioned.

According to the records management regulations developed by the National Archives and Records Administration, Adverse Action Files (AAF) should be destroyed no sooner than 4 years, but no later than 7 years after the case is closed.[14] An AAF is compiled when agencies impose an adverse or performance-based action against an employee and contains all the information related to the suspension or removal. OPFs and AAFs are maintained by the personnel department within the Office of Human Resources. We requested all 308 AAFs from the Agency, but 10 could not be located. Without proper documentation from the AAFs, the Agency does not have the evidence needed for due process.

[12] OMB Circular A-130, *Management of Federal Information Resources*, Revised (Transmittal Memorandum No. 4), section 7.h., page 5, November 30, 2000.

[13] Office of Personnel Management Operating Manual, *The Guide to Processing Personnel Actions*, April 6, 2003, section 1-3b(3), (as of March 9, 2004).

[14] National Archives and Records Administration, General Records Schedule 1 (Transmittal Memorandum No. 11), *Civilian Personnel Records*, Section 30.b, December 2003 (as of March 9, 2004).

CONCLUSIONS AND RECOMMENDATIONS

SSA, and particularly Operations, is proactive in its efforts to prevent and uncover potential employee systems security violations. This includes the establishment of policies and procedures, the development of the CIRP system, efforts to work with the OIG, and refresher training for the reviewers. While the Agency has integrity review policies and procedures in place, there are areas within the integrity review process that require improvement.

To strengthen SSA's integrity review process and reduce its vulnerability to employee systems security violations, we recommend SSA:

1. 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.

2. 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.

3. 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.

4. Continue to ensure all integrity reviews are conducted in a more timely and in-depth manner.

AGENCY COMMENTS AND OIG RESPONSE

In response to our draft report, SSA agreed with our recommendations and is in the process of implementing them. The Agency raised several points as other matters, which we have taken under consideration and incorporated where appropriate. We commend SSA for its efforts to protect the valuable information entrusted to the Agency and maintain the integrity of its workforce. See Appendix E for the text of SSA's comments.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

AAF	Adverse Action File
Act	The Social Security Act
CIRP	Comprehensive Integrity Review Process
CSI	Center for Security and Integrity
DSSPI	Division of Systems Security and Program Integrity
Handbook	Integrity Review Handbook
OI	Office of Investigations
OIG	Office of the Inspector General
OMB	Office of Management and Budget
Operations	Office of Operations
OPF	Official Personnel Folder
POMS	Program Operations Manual System
Sanctions	Sanctions for Unauthorized Systems Access Violations
SF-50	Notification of Personnel Action Form
SSA	Social Security Administration
SSN	Social Security Number
U.S.C.	United States Code

Background

The Privacy Act of 1974,[1] the Computer Fraud and Abuse Act,[2] the Computer Security Act of 1987,[3] the Office of Management and Budget Circulars A-123 and A-130, Appendix III, plus many other laws, guidelines and memoranda provide a body of regulations requiring the proper security of all automated information systems resources, including data.

The Privacy Act of 1974 prohibits the disclosure of personal information about an individual without prior written consent. Section 1106 of the Social Security Act (Act)[4] in accordance with the Computer Security Act of 1987 focuses on protecting the confidentiality of information in Government records. This section of the Act states that no file, record, report, paper, or other information obtained at any time from any person may be disclosed except as provided by regulations from the Act or other applicable laws.

In June 1998, the Social Security Administration (SSA) established a uniform set of *Sanctions for Unauthorized Systems Access Violations*[5] (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.

Managers are the primary lines of defense against employee systems security violations. SSA's Integrity Review Handbook outlines the procedures for managers when they conduct integrity reviews. In an effort to prevent and uncover potential employee systems security violations, SSA developed the Comprehensive Integrity Review Process (CIRP), a mainframe and Intranet based management tool to monitor specific SSA systems activity for potential fraud or misuse by employees. CIRP uses predetermined criteria to select certain queries input by employees and generates reports for review by management.

The manager determines whether the 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[6] must be contacted to

[1] 5 United States Code (U.S.C.) 552a (b).

[2] 18 U.S.C § 1030.

[3] Public Law 100-235.

[4] 42 U.S.C. § 1306.

[5] Information Systems Security Handbook, Chapter 21, Attachment: Commissioner's Memorandum, June 22, 1998.

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

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 for 7 years. The Audit Trail System is designed to provide SSA security officers with the capability to monitor SSA data entry activities nationwide.

PRIOR REVIEWS

- *Analysis of Social Security Number Misuse Allegations Made to the Social Security Administration's Fraud Hotline* (A-15-99-92019) dated August 1999. This report identified the different types of Social Security number (SSN) misuse allegations and estimated the number of occurrences for each category during the period of October 1, 1997 through March 13, 1999.

- *Referring Potentially Fraudulent Enumeration Applications to the Office of the Inspector General* (A-14-03-23052) dated March 2003. This report discussed the extent that SSA referred potentially fraudulent SSN applications to the OIG for investigation.

- *Management Advisory Report: Sensitive Data Accessible on the Social Security Administration Intranet* (A-14-04-24036) dated September 2003. This report identified sensitive personal information of OIG, SSA, State and contractor employees and beneficiaries improperly accessible on the Agency's Intranet.

We are currently performing audits of SSA's regional office procedures for addressing employee-related allegations in each of SSA's 10 regions. These audits include employee-related allegations of all types except systems security violations.

Scope and Methodology

Our objectives were to examine the processes that the Social Security Administration (SSA) has in place to review potential employee systems security violations in a timely and proper manner and to limit the Agency's exposure to employee misuse of its systems. We also examined the process used to refer violations to the Office of the Inspector General (OIG). Our review was based on the understanding that the Agency provided us with all the systems security violation cases for the regions selected and the period reviewed. Our analysis was limited by our reliance on the Agency's decision on whether a systems access was unauthorized and in violation of SSA's policies.

To meet our objectives, we examined reports of potential misuse or potential fraud employee systems security violations, as designated by SSA managers needing further review for all SSA components. We requested systems security violation sanction cases from all components Only the Office of Operations (Operations) provided sanction cases for review. They provided all the systems security violation cases that occurred between September 2000 and August 2003 in five regions (New York, Philadelphia, Dallas, Atlanta and San Francisco) and at SSA Headquarters. Other SSA Headquarter Offices provided information on potential systems security violations but had no actual sanction cases during that timeframe. While it is true that Operations has most of the employees with access to SSA's systems, it would seem unlikely that no employee in any other component has committed a systems security violation since 2000.

We received 308 cases from the 5 regions listed. For each case, we examined the Official Personnel Folder and the Adverse Action File to determine whether the Agency applied its sanction policy with consistency and timeliness. We compared all of these cases to the Office of Investigations' Allegation and Case Investigation System to determine whether these cases were referred to OIG for investigation. We confirmed the Social Security number or the name, regional location, and the time period of the offense. Additionally, we verified these cases with the five respective Centers for Security and Integrity (CSI) offices. We also:

1. Reviewed the following criteria:

   - Office of Management and Budget (OMB) Circular A-123, *Management Accountability and Control;*
   - OMB Circular A-130, *Management of Federal Information Resources;*
   - Office of Personnel Management and National Archives and Records Administration's guidance on personnel records;
   - SSA's Information Systems Security Handbook;
   - SSA's Program Operations Manual System; and
   - SSA's Integrity Review Handbook.

2. Interviewed representatives from SSA's:

- Operations, Office of Public Service and Operations Support, 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;
- Office of Systems, Integrity Systems Development Branch, to further understand the Comprehensive Integrity Review Process;
- Baltimore District Office to understand how SSA's policy and procedures were implemented in the local offices;
- Office of Central Operations CSI staff to understand the CSI's functions and role in the integrity review process; and
- Office of Labor Management and Employee Relations staff to understand the application of administrative sanctions in respect to systems security violations.

3. Visited the:

- Five regional offices listed previously, and
- The Baltimore Downtown District Office.

We reviewed the integrity review process for employee systems security violations for the entire Agency. We performed our field work in SSA Headquarters and selected regions from April 2003 to March 2004. 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.

Appendix D

Sanction Cases Reviewed for Systems Security Violations

Social Security Administration Region	Number of Cases Reviewed	Cases Referred to OIG by SSA				
		Offenses				
		Cat. I	Cat. IIA	Cat. IIB	Cat. III	Total
New York	76	0	0	0	0	0
Philadelphia	72	1	0	1	2	4
Atlanta	67	0	1	0	7	8
Dallas	45	1	1	0	0	2
San Francisco	48	1	0	0	2	3
Total	**308**	**3**	**2**	**1**	**11**	**17**

Appendix E

Agency Comments

SOCIAL SECURITY

MEMORANDUM 106-24-1067

Date: July 8, 2004 Refer To: S1J-3

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

From: Larry W. Dye /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "The Social Security Administration's Monitoring of Potential Employee System Security Violations" (A-14-04-23004)—INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report are attached.

Please contact me if you have any questions. Staff questions may be referred to Candace Skurnik, Director of the Audit Management and Liaison Staff, at extension 54636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL'S (OIG) DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S MONITORING OF POTENTIAL EMPLOYEE SYSTEM SECURITY VIOLATIONS" (A-14-04-23004)

Thank you for the opportunity to provide comments on this OIG draft report. We appreciate the report's recognition of the numerous processes in place at SSA for reviewing potential employee systems security violations, as well as the steps the Agency has taken to limit exposure to any violations. The actions cited in our comments demonstrate our ongoing commitment to making improvements in this important area, including continued cooperation with the OIG to address the issues raised in this OIG report.

Recommendation 1

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.

Recommendation 2

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.

Comment

We agree with the intent of recommendations 1 and 2, and we believe our present policies and procedures require reasonable retention of documentation necessary for ensuring effective resolution of and consistent application of sanctions for such cases. We will issue reminders as needed to management concerning these policies and procedures to assure that adequate documentation is maintained.

Recommendation 3

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.

Comment

We agree with this recommendation. Allowing OIG access to documentation concerning potential violations will allow OIG to assess the potential for criminal activity without unduly delaying local management's review of potential violations.

Currently, the SSA Office of Operations refers the cases listed below to OIG for review for possible investigation for criminal activity before any administrative action is taken on potential violation cases:

- All Category III cases (unauthorized access for personal gain or with malicious intent);
- All Category I cases (unauthorized access without disclosure); and
- Category IIA and Category IIB cases (unauthorized access with disclosure), where there exists, in management's opinion, possible criminal activity or intent.

The Agency will provide OIG's Office of Investigations (OI) six months of data for those cases where administrative action has already occurred. We have provided OI the requested information for the period January 2004 through March 2004. We will provide information for April 2004 through June 2004 in July 2004. Following review by OI, the SSA Office of Operations and OIG will reevaluate the referral process to determine if any modifications are necessary. We will also consider whether all potential sanctions cases should be referred to OIG prior to taking administrative action.

Recommendation 4

Continue to ensure all integrity reviews are conducted in a more timely and in-depth manner.

Comment

We agree with this recommendation, and recognize the importance of timely and thorough investigation and resolution of Comprehensive Integrity Review Process (CIRP) reviews. We currently devote significant amounts of time and resources to monitor accurate and timely completion of CIRP alerts.

[In addition to the items listed above, SSA also provided technical comments which have been addressed, where appropriate, in this report.]

Appendix F

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

Phil Rogofsky, Audit Manager, Network Security and Telecommunications Branch (410) 965-719

Acknowledgments

In addition to those named above:

Pat Kennedy, Audit Manager, Mainframe Controls and Advanced Techniques

Mary Ellen Fleischman, Senior Program Analyst

Harold Hunter, Senior Auditor

Greg Thompson, Senior Auditor

Grace Chi, Auditor

For additional copies of this report, please visit our web site at 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-14-04-23004.

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 Executive Operations (OEO). 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 Executive Operations

OEO supports OIG by providing information resource management and systems security. OEO also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OEO 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.