OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

REVIEW OF SOCIAL SECURITY ADMINISTRATION CONTROLS OVER THE ACCESS, DISCLOSURE AND USE OF SOCIAL SECURITY NUMBERS BY EXTERNAL ENTITIES

December 2002 **A-08-02-22071**

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: December 30, 2002 Refer To:

To: The Commissioner

From: Inspector General

Subject: Review of Social Security Administration Controls over the Access, Disclosure and Use of Social Security Numbers by External Entities (A-08-02-22071)

OBJECTIVE

Our objective was to assess the Social Security Administration's (SSA) controls over the access, disclosure and use of Social Security numbers (SSN) by external entities.

BACKGROUND

The SSN was created in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. However, over the years, the SSN has become a de facto national identifier used by Federal agencies, State and local governments, and private organizations. Government agencies frequently ask individuals for their SSNs because, in certain instances, the law requires them to or because SSNs provide a convenient means of tracking and exchanging information. While a number of laws and regulations require the use of SSNs for various Federal programs, they generally also impose limitations on how these SSNs may be used. Although no single Federal law regulates overall use and disclosure of SSNs by Federal agencies, the Freedom of Information Act of 1966, the Privacy Act of 1974, and the Social Security Act Amendments of 1990 generally govern disclosure and use of SSNs. See Appendix A for more information on the specific provisions of these laws.

Because of concerns related to perceived widespread sharing of personal information and occurrences of identity theft, Congress asked the General Accounting Office (GAO) to study how and to what extent Federal, State and local government agencies use individuals' SSNs and how these entities safeguard records or documents containing those SSNs.[1] As part of the study, GAO sent questionnaires to 18 Federal agencies (including SSA) that routinely collect, maintain, and use individuals' SSNs. Specifically, GAO's questionnaires asked each Federal agency to provide information about the following:

---

[1] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

- methods by which the agency obtains, maintains, and uses individuals' SSNs;
- practices for providing individuals' SSNs to other organizations; and
- practices for safeguarding records containing SSNs.

The information SSA and the other Federal agencies provided was self-reported, and GAO did not verify the responses. This report serves as a follow-up to GAO's study and provides a more in-depth analysis of SSA's controls over the access, disclosure and use of SSNs by external entities.

SCOPE AND METHODOLOGY

To accomplish our objective, we

- interviewed SSA Headquarters personnel responsible for controls over the access, disclosure and use of SSNs;
- reviewed relevant SSA procedures and practices;
- verified and updated key pieces of information SSA provided to GAO;
- reviewed applicable laws and regulations;
- observed selected contractor activities; and
- reviewed relevant audit reports.

Although SSA procedures and practices related to the access, disclosure and use of SSNs by external entities are virtually the same for all Agency programs, we focused our work on SSA's title II program. We selected this program, after consultation with SSA representatives, because it is the largest program for which SSA is responsible.

We performed our review at SSA Headquarters in Baltimore, Maryland, and a field office in Birmingham, Alabama. In addition, we interviewed personnel at three State Disability Determination Services (DDS) to assess their controls over contractors' access and use of SSNs.[2] We also visited five independent contractors in Birmingham, Alabama, to assess their controls for safeguarding SSN information.

The SSA entities reviewed were the Offices of the Deputy Commissioners for Finance, Assessment and Management; Disability and Income Security Programs; and Systems.

[2] In accordance with SSA disclosure regulations (20 CFR 401.25), SSA considers DDS personnel as SSA employees for purposes of accessing and re-disclosing personally identifiable information in SSA's possession when making disability determinations. Therefore, we consider DDS personnel as SSA employees for purposes of this report.

We conducted our audit from February through September 2002 in accordance with generally accepted government auditing standards.

RESULTS OF REVIEW

Although SSA has controls over the access, disclosure and use of SSNs by external entities, we are concerned about the Agency's exposure to improper SSN attainment and misuse. We identified instances in which SSA personnel unnecessarily displayed SSNs on documents it sent to external entities that may not have had a need to know. In addition, we identified instances in which SSA personnel were not adequately monitoring contractors' access and use of SSNs. Furthermore, based on our review of recent audit reports related to SSA's information security environment, the Agency may be vulnerable to unauthorized access to its computer systems containing SSNs.

SSA Makes Legal and Informed Disclosures But Unnecessarily Displays SSNs on Certain Documents it Sends to External Entities

SSA generally makes proper SSN disclosure to external entities. SSA personnel inform numberholders of whether they must provide their SSN to apply for benefits and, if so, how the Agency will use the SSN. We did not identify any specific instances involving improper disclosure of SSNs. Moreover, according to attorneys with SSA's Office of General Counsel, the Agency has not been party to any litigation regarding improper SSN disclosure.

SSA's disclosure policy allows for the release of individuals' SSNs to external entities as necessary to administer its programs under the Social Security Act. SSA releases SSNs with the numberholder's written consent and in other situations where Federal law authorizes disclosure. Examples include disclosure of SSNs in the following circumstances.

- To Federal, State and local governments that are authorized under Federal law to collect and use SSNs to administer income and health maintenance programs. For example, the Department of Veterans Affairs uses SSNs to administer its veterans pension and compensation programs.

- To prison systems because Federal law requires that they report prison information to SSA.

- To States' vital records and statistics agencies for administering public health and income maintenance programs, including statistical studies and evaluation projects.[3]

While delivering services and benefits, SSA, like many Federal agencies, displays SSNs on documents that may be viewed by others, some of whom may not have a need to know. We identified instances in two States in which DDS personnel

[3] *Master Files of SSN Holders and SSN Applications*, SSA/OSR, 60-0058.

unnecessarily displayed SSNs on documents it sent to third parties. DDS personnel routinely send questionnaires to third parties (for example, neighbors or friends) requesting information about disability claimants' daily activities. We question whether individuals receiving these questionnaires need to know a disability claimant's SSN. We also identified instances in which SSA personnel displayed SSNs on forms it sent to vocational experts (independent contractors) requesting opinions about disability claimants' ability to work. We question whether these third parties need to know a disability claimant's SSN.

We believe displaying SSNs on documents sent to individuals who may not have a need to know increases the risk that others may improperly obtain and misuse the SSN. In fact, personnel in one State DDS told us they recognized the vulnerability associated with displaying SSNs on third-party questionnaires and changed to a case numbering system to assist them in identifying claimant files.

SSA Places Safeguard Requirements on Contractors But Lacks Adequate Monitoring

SSA and State DDSs award thousands of contracts, acquisitions, and orders each year. Examples of contractors who use files and other information that may contain SSNs include doctors (that is, panel physicians) who perform medical examinations for disability determinations and vocational experts who provide opinions to SSA Offices' of Hearings and Appeals.

SSA's disclosure policy allows SSA to provide SSNs to contractors as necessary to assist the Agency in carrying out its statutory responsibilities.[4] Contracts generally contain standard language related to personal information safeguards, including the SSN, which SSA requires contractors to follow. Contracts may also contain penalty provisions for misuse of information by contractors. SSA places numerous requirements regarding the privacy of SSNs on contractors. For example, entities receiving SSN information (1) cannot provide it to other entities, (2) cannot allow any unauthorized persons to see individuals' SSNs, and (3) must keep records containing SSNs in a secure place.

To determine whether SSA had appropriate controls over contractors' access to, and use of, SSNs, we reviewed monitoring site visit reports and checklists, observed security practices at contractors' offices, and examined a written agreement. Our review of SSA's formal and informal site visit reports found that personnel did not address the security of personal identifying information, such as SSNs, during monitoring visits. Our review of the monitoring checklist State DDS personnel use when conducting contractor site visits, which conforms to SSA guidelines,[5] does not address the security of personal identifying information. Given the importance of preventing

[4] Ibid.

[5] Program Operations Manual System, DI 39545.900.

improper attainment and misuse of SSNs, we believe SSA's monitoring activities should include an evaluation of contractors' security practices to ensure they uphold their obligation to protect the confidentiality and security of SSNs.

Based on our discussions and observations at panel physicians' offices, we are also concerned about controls over contractors' security practices for file storage. For example, we noted instances in which physicians maintained personal identifying information, including SSNs, in unlocked file cabinets or storage rooms, neither of which provided adequate security. State DDS personnel who accompanied us on our site visits shared our concern of inadequate file security.

The agreement with Consulting Professionals and Hospitals or Clinics (panel physicians) we reviewed includes language that prohibits "unauthorized disclosure of information." The agreement also addresses potential third-party providers who may provide needed assistance, such as transcription services. The agreement requires panel physicians to inform a third-party "that services are being performed in connection with a Social Security program, and that improper disclosure of information about the subject individual is prohibited." Panel physicians we interviewed told us they had not discussed security of personal identifying information, such as SSNs, with transcription services personnel, as required by their agreement with SSA. In addition, although the Blanket Purchase Agreement SSA uses for vocational experts incorporates the Privacy Act by reference, we encourage SSA to add specific SSN disclosure language for emphasis, as it uses in other SSA contracts.

SSA Places Controls over Access to Individuals' SSNs Maintained in its Databases, But Weaknesses Exist

Although SSA limits access to its databases primarily to its employees, the Agency also authorizes systems access to external entities for specific purposes. For example, SSA allows agencies, such as the Centers for Medicare and Medicaid Services and the Railroad Retirement Board access to its databases to assist in beneficiary eligibility determinations. SSA also allows contractors access to its databases to provide such services as software design and support and data processing.

Federal laws lay out a framework for Federal agencies to follow when establishing information security programs that protect sensitive personal information, such as SSNs.[6] This framework includes four principles that are important to an overall information security program. These principles are to periodically assess risk, implement policies and controls to mitigate risks, promote awareness of risks for information security, and continually monitor and evaluate information security practices. To gain a better understanding of whether SSA had in place measures to adequately safeguard SSNs that are consistent with the Federal framework, we

[6] See the Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988); the Paperwork Reduction Act of 1995, Pub. L. No. 104-13, 109 Stat. 163 (1995); the Clinger-Cohen Act of 1996, Pub. L. No. 104-106 § 4304, 110 Stat. 186, 659 (1996); and OMB guidance, such as Circular A-130.

reviewed recent audit reports related to its information security environment. See Appendix B for a list of audit reports related to SSA's information security environment.

SSA's information security framework includes self-reviews and policies and procedures to safeguard its sensitive information systems. For example, SSA conducts annual self-reviews on its sensitive systems to certify that adequate controls exist.[7] In addition, SSA formed a Security Response Team to address security incidents involving its computer systems, Internet and Intranet servers, and Local Area Network[8] servers. To detect systems violations, SSA uses such tools as integrity reviews, audit trail systems, and access controls. Furthermore, to better coordinate and monitor its Agency-wide security framework, SSA recently established the Office of the Chief Information Officer to centralize system security policies and procedures.

We acknowledge SSA has made strides in its information security efforts. However, despite SSA's controls, recent Office of the Inspector General and contractor audit reports identified weaknesses within its information security environment. Main areas of vulnerability include the following:

- physical access controls at non-Headquarters locations, including SSA's regional offices, program service centers, and selected DDSs;

- implementation and monitoring of technical security configuration standards governing systems housed in the National Computer Center and off-site house systems; and

- monitoring security violations and periodic review of user access.[9]

Because of the sensitive nature of information security issues, we chose to withhold detailed descriptions of information security control weaknesses identified in recent audit reports. We are working with SSA to reach consensus on an effective action plan to resolve these weaknesses.

CONCLUSION AND RECOMMENDATIONS

Despite SSA's safeguards to prevent improper access, disclosure and use of SSNs by external entities, the Agency remains at-risk to such activity. We recognize SSA's efforts can never eliminate the potential that unscrupulous individuals may

---

[7] *Social Security: Annual Program Review Government Information Security Reform Act*, September 2002, pp. 3-4.

[8] A Local Area Network or LAN is a system for linking programs, storage, and devices to multiple workstations over an area such as, within a building.

[9] *Social Security Administration Performance and Accountability Report for Fiscal Year 2001*, December 2001, pp. 225-226.

inappropriately acquire and misuse SSNs. Nonetheless, we believe SSA, as a Federal agency and public servant, has a duty to safeguard the integrity of SSNs by reducing opportunities for external entities to improperly obtain and misuse the SSNs. Given the potential risk for individuals to engage in such activity, we believe SSA would benefit by strengthening some of its controls over the access, disclosure and use of SSNs by external entities.

Accordingly, we recommend that SSA:

1. Limit SSN display on documents to external entities to those that have a need to know.

2. Monitor contractors' access, disclosure and use of SSNs to ensure they uphold their obligation to protect the confidentiality and security of SSNs.

3. Continue to address identified weaknesses within its information security environment to better safeguard SSNs.

AGENCY COMMENTS

SSA agreed with our recommendations. Regarding Recommendation 1, SSA agreed that SSNs should not be used on documents sent to external entities that do not have a need to know the SSN. SSA plans to issue a reminder to the DDSs regarding adherence to policy and procedural instructions that govern the display of SSNs on correspondence. Regarding Recommendation 2, SSA stated it plans to add specific SSN disclosure language in its contracts/Blanket Purchase Agreements by the end of Fiscal Year 2003. SSA also stated it plans to issue a reminder to State DDSs to re-emphasize the serious responsibility to monitor and protect the confidentiality and security of SSNs disclosed to contractors and revise site visit instructions to include specific reference to monitoring the security of the information. Regarding Recommendation 3, SSA stated it will continue to work with the OIG to reach consensus on an effective action plan to resolve identified information security weaknesses. The full text of SSA's comments is included in Appendix C.

James G. Huse, Jr.

Appendices

Federal Laws that Restrict Disclosure of the Social Security Number

The following Federal laws establish a framework for restricting Social Security number (SSN) disclosure.[1]

The Freedom of Information Act (5 U.S.C. 552)

The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of Executive Branch agencies and departments are accessible to the people. FOIA, as amended, provides that the public has a right of access to Federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the Government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to State and local governments.

The Privacy Act of 1974 (5 U.S.C. 552a)

The Privacy Act regulates Federal agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records. The Act prohibits the disclosure of any record contained in a system of records unless the disclosure is made based on a written request or prior written consent of the person to whom the records pertain or is otherwise authorized by law. The Act authorizes 12 exceptions under which an agency may disclose information in its records.

The Act contains a number of additional provisions that restrict Federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or Executive Order of the President, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under Federal programs.

[1] Summarized from *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii))[2]

The Social Security Act bars disclosure by Federal, State and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the act also contains criminal penalties for "unauthorized willful disclosures" of SSNs. Because the Act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by Federal entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear if the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to Federal, State and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

[2] Pub. L. No. 101-624 §2201, 104 Stat. 3359, 3951 (1990).

Reports Related to the Social Security Administration's Information Security Environment

The Social Security Administration's Office of the Inspector General

General Controls of the Alabama Disability Determination Services Claims Processing System Need Improvement, A-14-02-22089, September 2002.

The Social Security Administration's Compliance with the Government Information Security Reform Act, A-14-02-12042, September 2002.

Review of Security over Remote Access to the Social Security Administration's Main Processing Environment, A-14-01-11010, May 2002.

Disclosure of Personal Beneficiary Information to the Public, A-01-01-01018, January 2002.

Management Advisory Report: Implementation of the Government Information Security Reform Act, A-14-01-21056, September 2001.

The Social Security Administration's Compliance with the Government Information Security Reform Act, A-14-01-21055, September 2001.

Audit of the Administrative Costs Claimed by the Connecticut Disability Determination Services, A-15-00-30016, September 2001.

Social Security Administration's Intelligent Work Station/Local Area Network and Telecommunication Security, A-14-99-11005, August 2001.

Management Advisory Report - Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulation, A-13-98-12044, June 2001.

Management Advisory Report – Administration of TOP SECRET at the National Computer Center, A-14-99-11001, September 2000.

Social Security Administration's Suitability Program for Employees and Contractors, A-14-99-12006, June 2000.

PricewaterhouseCoopers LLP

Social Security Administration's Fiscal Year 2001 Audit/Management Letter Part 1, November 2001.

Janus Associates, Inc.

SSA-63 Task 1 Penetration Testing for Social Security Administration, March 2001.

Deloitte & Touche

Social Security Administration National Computer Center Likelihood Report (Contract No. 600-98-34387), July 2001.

Title II Redesign, Release One (Contract No. 600-98-34387), June 2001.

Department of the Treasury, Internal Revenue Service

Safeguard Review Report (Catalog No. 45306Z), January 2000.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: December 16, 2002 Refer To: S1J-3

To: James G. Huse, Jr.
Inspector General

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

Subject: Office of the Inspector General Draft Report, "Review of Social Security Administration Controls over the Access, Disclosure and Use of Social Security Numbers by External Entities (A-08-02-22071)—INFORMATION

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

Please let us know if we can be of further assistance. Staff questions can be referred to Laura Bell on extension 52636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "REVIEW OF SOCIAL SECURITY ADMINISTRATION CONTROLS OVER THE ACCESS, DISCLOSURE AND USE OF SOCIAL SECURITY NUMBERS BY EXTERNAL ENTITIES" (A-08-02-22071)

As OIG is aware, we have long been concerned about ensuring the confidentiality of all personal information maintained by the Agency. We already have established policies, procedures and technical configurations standards requirements.

To safeguard our sensitive information systems, we have included self-reviews, policies and procedures in our information security framework. In addition, we monitor technical configuration standards of systems throughout the Agency and perform systems security reviews and audits periodically throughout the year. We have established a Security Response Team (SRT) to address security incidents.

On a quarterly basis, we examine, audit and review audit conclusions and recommendations to determine the progress we have made toward closure of the issues.

We are actively reviewing access at component levels, and will continue to monitor security violations and periodic reviews of user access. We are working with OIG to establish an acceptable review and control process for access at all component levels. For the Disability Determination Services in the states, we have developed and distributed a security document and continue to work with them to ensure compliance with established policies, procedures, and configuration standards.

We also actively monitor network activity for anomalies and have a real-time emergency notification program. The notification program provides continuous coverage and responds to any threats and vulnerabilities.

With the policies, procedures, configuration standards, and monitoring activity presently in place and the addition of improved technologies/processes as they are available, we will continue to make strides in our information security efforts.

Our responses to the specific recommendations are provided below.

Recommendation 1

Limit Social Security Number (SSN) display on documents to external entities to those that have a need to know.

Comment

We agree that SSNs should not be used on documents sent to external entities that do not have a need to know the SSN. We have policy and procedural instructions in place (POMS GN 03325.005, GN 03325.020) that govern the display of SSNs on correspondence. We will issue a reminder to the Disability Determination Services (DDS) regarding adherence to the policy and instructions.

Recommendation 2

Monitor contractors' access, disclosure and use of SSNs to ensure they uphold their obligation to protect the confidentiality and security of SSNs.

Comment

We agree with the recommendation to the extent that it applies to contracts and contractor performance for which the Agency has responsibility, including the addition of specific SSN disclosure language to the Blanket Purchase Agreements (BPA) that the Office of Hearings and Appeals (OHA) awards to Medical and Vocational Experts. We plan to add the specific SSN disclosure language in the several-thousand contracts/BPAs before the end of this fiscal year.

As for OIG's observations regarding contracts awarded by the State DDSs, these contracts are not subject to SSA's acquisition policy or to the Federal Acquisition Regulation. We will issue a reminder to the States to re-emphasize the serious responsibility to monitor and protect the confidentiality and security of SSNs and personal identity information disclosed to their contractors, and will revise the site visit instructions to include specific reference to monitoring the security of the information.

Recommendation 3

Continue to address identified weaknesses within the Agency's information security environment to better safeguard SSNs.

Comment

We will continue to work with OIG, as noted in the report, to reach consensus on an effective action plan to resolve the identified weaknesses.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Jeff Pounds, Acting Director, Southern Audit Division, (205) 801-1606

Staff Acknowledgments

In addition to the persons named above:

Kathy L. Youngblood, Auditor-in-Charge

Theresa Roberts, Auditor

Kimberly Beauchamp, Writer/Editor

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-08-02-22071.

DISTRIBUTION SCHEDULE

	No. of Copies
Commissioner of Social Security	1
Management Analysis and Audit Program Support Staff, OFAM	10
Inspector General	1
Assistant Inspector General for Investigations	1
Assistant Inspector General for Executive Operations	3
Assistant Inspector General for Audit	1
Deputy Assistant Inspector General for Audit	1
Director, Data Analysis and Technology Audit Division	1
Director, Financial Audit Division	1
Director, Southern Audit Division	1
Director, Western Audit Division	1
Director, Northern Audit Division	1
Director, General Management Audit Division	1
Team Leaders	25
Income Maintenance Branch, Office of Management and Budget	1
Chairman, Committee on Ways and Means	1
Ranking Minority Member, Committee on Ways and Means	1
Chief of Staff, Committee on Ways and Means	1
Chairman, Subcommittee on Social Security	2
Ranking Minority Member, Subcommittee on Social Security	1
Majority Staff Director, Subcommittee on Social Security	2
Minority Staff Director, Subcommittee on Social Security	2
Chairman, Subcommittee on Human Resources	1
Ranking Minority Member, Subcommittee on Human Resources	1
Chairman, Committee on Budget, House of Representatives	1
Ranking Minority Member, Committee on Budget, House of Representatives	1
Chairman, Committee on Government Reform and Oversight	1
Ranking Minority Member, Committee on Government Reform and Oversight	1
Chairman, Committee on Governmental Affairs	1

Ranking Minority Member, Committee on Governmental Affairs	1
Chairman, Committee on Appropriations, House of Representatives	1
Ranking Minority Member, Committee on Appropriations, House of Representatives	1
Chairman, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives	1
Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives	1
Chairman, Committee on Appropriations, U.S. Senate	1
Ranking Minority Member, Committee on Appropriations, U.S. Senate	1
Chairman, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate	1
Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate	1
Chairman, Committee on Finance	1
Ranking Minority Member, Committee on Finance	1
Chairman, Subcommittee on Social Security and Family Policy	1
Ranking Minority Member, Subcommittee on Social Security and Family Policy	1
Chairman, Senate Special Committee on Aging	1
Ranking Minority Member, Senate Special Committee on Aging	1
President, National Council of Social Security Management Associations, Incorporated	1
Treasurer, National Council of Social Security Management Associations, Incorporated	1
Social Security Advisory Board	1
AFGE General Committee	9
President, Federal Managers Association	1
Regional Public Affairs Officer	1
Total	**96**

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) provides four functions for the Office of the Inspector General (OIG) – administrative support, strategic planning, quality assurance, and public affairs. OEO supports the OIG components by providing information resources management; systems security; and the coordination of budget, procurement, telecommunications, facilities and equipment, and human resources. In addition, this Office coordinates and is responsible for the OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act. The quality assurance division performs internal reviews to ensure that OIG offices nationwide hold themselves to the same rigorous standards that we expect from the Agency. This division also conducts employee investigations within OIG. The public affairs team communicates OIG's planned and current activities and the results to the Commissioner and Congress, as well as other entities.

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.