United States General Accounting Office

GAO

Report to Congressional Requesters

September 2003

SOCIAL SECURITY ADMINISTRATION

Disclosure Policy for Law Enforcement Allows Information Sharing, but SSA Needs to Ensure Consistent Application

GAO-03-919

September 2003

SOCIAL SECURITY ADMINISTRATION

Disclosure Policy for Law Enforcement Allows Information Sharing, but SSA Needs to Ensure Consistent Application

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-919, a report to congressional requesters

Why GAO Did This Study

Law enforcement agencies' efforts to investigate the events of September 11th increased awareness that federal agencies collect and maintain personal information on individuals such as name, social security number, and date of birth that could be useful to law enforcement. The Social Security Administration (SSA) is one of the country's primary custodians of personal information. Although the Privacy Act protects much of this information, generally, federal agencies can disclose information to law enforcement. However, determining when the need for disclosure takes priority over an individual's privacy is not clear. GAO was asked to describe (1) SSA's disclosure policy for law enforcement and how it compares with the Privacy Act and those of other federal agencies, (2) SSA's experience sharing information with law enforcement, and (3) law enforcement's experience obtaining information under SSA's policy.

What GAO Recommends

GAO recommends that the SSA Commissioner take steps (1) to ensure that its policy is consistently applied across all offices and (2) to provide information on the disclosure policy and procedures to law enforcement entities at all levels of government. SSA raised some concerns but generally agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-919.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Barbara Bovbjerg, 202-512-7215, bovbjergb@gao.gov.

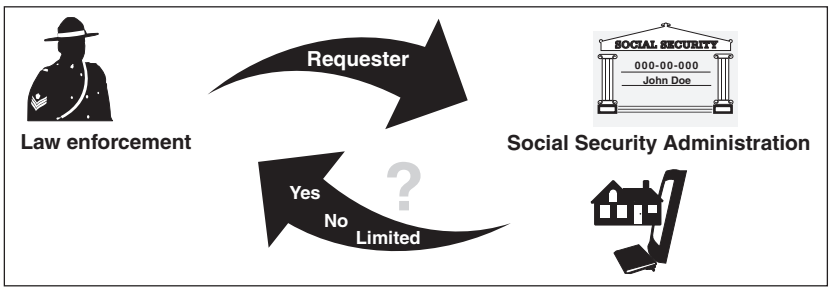
What GAO Found

Although SSA's disclosure policy permits the sharing of information with law enforcement entities, it is more restrictive than the Privacy Act and the disclosure policies of most federal agencies. While the Privacy Act permits disclosures to law enforcement for any type of crime, SSA only allows disclosures under certain conditions. For example, for serious and violent crimes, SSA will disclose information to law enforcement if the individual whose information is sought has been indicted or convicted of that crime. Even when information is disclosed, it might be limited to results obtained from verifying a social security number and name unless the investigation concerns fraud in SSA or other federal benefit programs, then the agency can work with law enforcement officials as part of a task force or joint investigation. However, the disclosure policies for law enforcement of the Internal Revenue Service (IRS) and the Census Bureau, both of which have requirements prescribed in their statutes, are also more restrictive than the Privacy Act and the policies of most federal agencies. SSA officials consider SSA's disclosure policy integral to carrying out the agency's mission.

The various restrictions in SSA's disclosure policy create a complex policy that is confusing and could cause inconsistent application across the agency's more than 1,300 field offices. This could result in uneven treatment of law enforcement requests. Because aggregated data were not available, GAO was unable to assess the extent to which SSA does not consistently apply its policy. However, GAO was told of instances in which SSA officials in some field offices did not give law enforcement information that appeared to be permitted under the policy as well as instances in which they gave them more than what appeared to be allowed.

Generally, law enforcement officials find the limited information SSA shares useful to their investigation, but many law enforcement officials, particularly state and local law enforcement officials, are not familiar with the policy or the process for requesting information from SSA. Most law enforcement officials expressed a desire for more information than is currently permitted under SSA's policy, but SSA maintains that providing more information would hurt its ability to carry out its primary mission.

Personal Information SSA Discloses



Sources: GAO and copyright © Corel Corp. All rights reserved.

Contents

Letter 1

Results in Brief 2
Background 4
SSA's Disclosure Policy Allows Information Sharing with Law Enforcement under Certain Conditions, but is More Restrictive than the Privacy Act 7
SSA Has Provided Information to Law Enforcement Officials, but Confusion about the Disclosure Policy May Cause Inconsistent Application 20
While Some Law Enforcement Officers Were Unfamiliar with the Policy, Most Were Generally Satisfied with the Information Shared 24
Conclusions 27
Recommendations 28
Agency Comments and Our Evaluation 28

Appendix I **Scope and Methodology** 32

Appendix II **Chief Financial Officers' Act Agencies' Rules on Disclosure of Records to Law Enforcement** 35

Appendix III **Comments from the Social Security Administration** 36

Appendix IV **GAO Contacts and Staff Acknowledgments** 41

GAO Contacts 41
Staff Acknowledgments 41

Tables

Table 1: Exceptions Permitted under the Privacy Act for Disclosing Information 6
Table 2: Number of Information Requests Granted to Law Enforcement by OIG Field Divisions and Headquarters in Fiscal Years 2000 through 2002 24

Figure

Figure 1: SSA's Disclosure Policy for Law Enforcement 12

Abbreviations

CD-ROM	Compact Disc-Read-Only Memory
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
FR	Federal Register
ICE DHS	Immigration and Customs Enforcement Department of Homeland Security
INS	Immigration and Naturalization Service
IRC	Internal Revenue Code
IRS	Internal Revenue Service
MOU	memorandum of understanding
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POMS	Program Operations Manual System
SSA	Social Security Administration
SSI	Supplemental Security Income
SSN	Social Security number
USC	United States Code

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

September 30, 2003

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
House of Representatives

The Honorable E. Clay Shaw, Jr.
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Law enforcement agencies' efforts to investigate the events of September 11th increased awareness that federal agencies collect and maintain personal information on individuals that could be useful to law enforcement in helping them locate and prosecute individuals responsible for crimes. Federal agencies maintain personal information such as name, social security number (SSN), and address in their databases. For example, the Social Security Administration (SSA), the federal agency responsible for administering three major benefit programs and issuing SSNs, is one of the country's primary custodians of personal information, maintaining records on 290 million living individuals. To protect personal information collected by all federal agencies, including SSA, the Congress passed the Privacy Act in 1974. The Privacy Act generally requires the individual affected to give consent before a federal agency discloses personal information the agency maintains in certain records and retrieves using the individual's name or other identifying information. However, there are 12 exceptions to the restrictions placed on federal agencies for disclosing this personal information, one of which permits disclosure to law enforcement agencies as long as certain criteria are met.

The Privacy Act protects individuals' privacy while, at the same time, allowing individuals' personal information to be disclosed for appropriate purposes, such as assisting law enforcement. Determining when the need for disclosure takes priority over an individual's privacy is not always clear. With an eye toward finding an appropriate balance between protection and disclosure of personal information, the Congress asked us to describe: (1) SSA's disclosure policy for law enforcement purposes and how it compares to the Privacy Act and other federal agencies, (2) SSA's experience sharing information with law enforcement agencies, and

(3) law enforcement's experience in obtaining information under SSA's disclosure policy.

To provide information on these issues, we compared SSA's disclosure policy for law enforcement with the Privacy Act and with disclosure policies of the other 23 federal agencies covered by the Chief Financial Officers' Act. Because the Internal Revenue Service (IRS) and the Bureau of the Census, like SSA, are similar in size and scope of data maintained on individuals, we also compared SSA's disclosure policy with those of IRS and Census. We also made site visits and interviewed officials about their experiences with SSA's disclosure policy at SSA headquarters; SSA regional and field offices; SSA's Office of the Inspector General (OIG); and federal, state, and local law enforcement agencies. In addition, we surveyed a random sample of SSA field offices and all SSA OIG field offices for investigations to obtain information on law enforcement requests and disclosures between fiscal years 1999 and 2002. The information provided by all entities was self-reported. We conducted our work between August 2002 and July 2003 in accordance with generally accepted government auditing standards. For additional information on our scope and methodology, see appendix I.

Results in Brief

While SSA's policy permits the sharing of information with law enforcement under certain conditions, it is more restrictive than the law enforcement exception specified under the Privacy Act and the policies of most federal agencies. SSA's disclosure policy requires SSA officials to consider several factors such as the nature of the alleged criminal activity of the individual on whom information is requested, what information has been requested, and which agency has made the request. These requirements stem from a confidentiality policy established in 1937 that prohibited most disclosures. SSA is also the custodian of tax information, which can only be disclosed as permitted in the Internal Revenue Code (IRC). With regard to nontax information, SSA modified its policy subsequent to the enactment of the Privacy Act, to permit disclosures, but only for certain types of crimes or under certain conditions. For example, the Privacy Act allows the sharing of information on individuals who are the subjects of criminal investigations regardless of the type of crimes but under SSA's policy, if the type of crime is considered violent and serious, individuals must have been indicted or convicted of the crime before information is shared. SSA maintains that it must have a restrictive disclosure policy because much of the information the agency maintains was initially obtained under a pledge of confidentiality. Unlike SSA, the policies of most major federal agencies allow the disclosure of information

to law enforcement if the requests for information meet the requirements outlined in the Privacy Act. However, the disclosure policies of IRS and Census—two agencies that also maintain information on millions of individuals—have disclosure requirements prescribed in their statutes that are also more restrictive than the Privacy Act and the policies of most federal agencies. The IRS statute prohibits disclosing certain taxpayer information to other federal departments and agencies without specific statutory authorization. The Census Bureau's statute does not authorize any disclosures of individual census data to law enforcement.

Although SSA's policy supports sharing tax information as permitted by the IRC and limited nontax information with law enforcement under certain conditions, some SSA field office staff appear confused about the policy and may be applying it inconsistently. Law enforcement can request information from any SSA field office, including OIG offices. On the basis of our random sample of field offices, we estimate that 82 percent of these offices received requests for personal information from law enforcement agencies. The information most frequently shared was the result of name and SSN verification. Through our site visits and survey results, we were told about both instances in which it appeared that SSA field offices denied law enforcement requests when they could have provided information and instances in which it seemed that offices provided more information than was permitted under SSA's policy.

While some law enforcement officials were unfamiliar with SSA's disclosure policies, most were generally satisfied with the information provided by SSA, though most wanted more. Some law enforcement agencies at the state and local level were unfamiliar with the process for obtaining information and expressed frustration. These law enforcement agencies frequently were unfamiliar with the process for obtaining information until after making initial requests to SSA field offices and, in some instances, they told us that they had their requests turned down because they did not follow procedures. Federal law enforcement agencies, on the other hand, were more familiar with the procedures for obtaining information from SSA. Law enforcement officials at all levels indicated that the SSN and name verification SSA provided was often helpful to their investigations. However, most wanted SSA to provide additional information such as address, date of birth, and employer or family information. Some law enforcement officers told us that they wanted SSA to expand the circumstances under which disclosures could be made. However, SSA officials expressed concern that expanding SSA's disclosure policy would hamper the agency's ability to ensure that

individuals' personal information is protected and that resources are not diverted from administering Social Security benefit programs.

We make recommendations in this report that the Commissioner of SSA take steps to ensure consistent application of the disclosure policy for law enforcement in all of the agency's offices and better assist law enforcement agencies making requests, so that they understand the procedures for making requests.

In its comments on a draft of this report, SSA raised some concerns, but generally agreed with our recommendations and believed in some instances, the agency was already taking steps to address the issues we raised. However, SSA expressed concern that our draft report did not completely describe the statutory basis and rationale behind SSA's disclosure policy, and therefore our findings and recommendations are "overbroad". We believe our findings and recommendations are well grounded; however, we have made some clarifications in this report in response to SSA's comments.

Background

With virtually billions of records, the federal government is the largest single producer, collector, and user of information in the United States. In order to carry out the various missions of the federal government, federal agencies collect and maintain personal information such as name, date of birth, address, and SSNs to distinguish among individuals and ensure that people receive the services or benefits they are entitled to under the law. SSA is responsible for issuing SSNs as part of its responsibility for administering three major income support programs for the elderly, disabled, and their dependents: the Old-Age and Survivors Insurance; Disability Insurance; and Supplemental Security Income. SSA is also the repository of information on individuals' wages and earnings. This information is used in tax administration and is reported by individuals on their federal income tax returns. Tax return information may only be disclosed as permitted by the IRC.

Information transmitted to SSA has been protected from disclosure by statute and regulation since the inception of the Social Security program. To maintain the confidentiality of the personal information the agency collects to carry out its mission, in June 1937, SSA adopted its first regulation, known as "Regulation No. 1," to protect the privacy of individuals' records and to include a pledge of confidentiality. The regulation was reinforced by amendments to the Social Security Act in 1939, which became the statutory basis for maintaining the confidentiality

of SSA's records. For decades, the act, along with Regulation No. 1, formed the basis for SSA's disclosure policy.[1] However, the enactment of subsequent legislation—the Freedom of Information Act (FOIA) in 1966[2] and Government in the Sunshine Act in 1976—caused SSA to reexamine its disclosure and confidentiality policy. This legislation placed the burden on SSA, as well as other federal agencies, to justify withholding information requested. Still, SSA's policy is designed to protect the privacy rights of individuals to the fullest extent possible while permitting the exchange of records required to fulfill its administrative and program responsibilities. Over the years, SSA's disclosure policy has been revised to comply with about 25 statutes, including the Privacy Act.

The Privacy Act of 1974 is the primary law governing the protection of personal privacy by agencies of the federal government.[3] The Privacy Act regulates the collection, maintenance, use, and disclosure of personal information that federal agencies maintain in a system of records.[4] The act requires that, at the time the information is collected, agencies inform an individual of the following: (1) authority for the collection and whether it is mandatory or voluntary, (2) the principal purpose for the collection of information, (3) what the routine uses for the information may be, and (4) what the consequences are of not providing the information.[5] The act applies to systems of records maintained by federal agencies, and with certain exceptions, prohibits agencies from disclosing such records without the consent of the individual whose records are being sought. The act authorizes 12 exceptions under which a federal agency may disclose information in its records without consent, as shown in table 1. The Privacy Act requires that the Office of Management and Budget (OMB) issue guidance and oversee agency implementation of the act. The act does not generally apply to state and local government records; state laws

[1]This statute is codified at 42 U.S.C. 1306.

[2]FOIA provided the public a right of access to federal agency records unless they are protected from disclosure by nine stated exemptions.

[3]Generally applicable privacy-related requirements are also found in the FOIA, the Paperwork Reduction Act of 1995, and the E-Government Act of 2002, among others.

[4]The Privacy Act defines a system of records as a group of records containing information about individuals under the control of the agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual, such as an SSN.

[5]Agencies are required to publish notices in the *Federal Register* concerning the establishment and revision of systems of records and to ensure the security and confidentiality of the information in those systems.

vary widely regarding disclosure of personal information in state government agencies' control.

Table 1: Exceptions Permitted under the Privacy Act for Disclosing Information

Activity or agency warranting exception	Conditions under which disclosure is permitted
1. Internal use within federal agency	If an employee or officer of the agency maintaining the record needs the information to perform official duties.
2. FOIA	If the provisions of the FOIA require the disclosure.
3. Routine use[a]	If the use has been determined to be compatible with the purpose for which the data were originally collected.[b]
4. Census Bureau	For planning or conducting a census, survey, or related activity authorized by the Census statute.
5. Statistical research	If written assurance is provided that the record would be used solely as a statistical record and it is transferred in a form that personal information will not be individually identifiable.
6. National Archives	If the record has sufficient historical or other value to warrant its evaluation for preservation by the Archivist of the United States or a designee.
7. Civil or criminal law enforcement	If used for the purpose of a civil or criminal law enforcement activity within the United States.
8. Health or safety	If compelling circumstances affect the health or safety of an individual.[c]
9. Congress	If either house of the Congress or committees or subcommittees with jurisdiction over the subject requests disclosure.
10. Comptroller General	If disclosure is for use in the performance of the duties of the General Accounting Office.
11. Court order	If pursuant to the order of a court of competent jurisdiction.
12. Consumer reporting agency	If disclosure is relevant to collection of a claim of the United States Government (31 USC 3711(e)).

Source: GAO review of the Privacy Act.

[a]Agencies must keep an accounting of disclosures made under exceptions 3-12.

[b]The routine use must have been publicly identified (in the *Federal Register*) as such prior to disclosure.

[c]The Privacy Act requires that the individual be notified after the disclosure is made.

The Privacy Act, under the law enforcement exception, outlines the minimum criteria that must be met by a law enforcement agency to obtain personal information without an individual's consent. The act requires that

the request specify the information being sought and the law enforcement activity being carried out. The request must be in writing, and signed by the agency head.[6] In addition, OMB guidance permits agencies to disclose a personal record covered by the Privacy Act to law enforcement at the agencies' own initiative, when a violation of law is suspected; provided that such disclosure has been established in advance as a "routine use" and misconduct is related to the purposes for which the records are maintained. The routine use exception of the Privacy Act permits disclosure of individuals' personal information if the requested use is compatible with the purpose for which the information was initially collected.

Under the act, agencies are required to keep an accurate accounting regarding each disclosure of a record to any person or to another agency and to retain the accounting for at least 5 years or the life of the record, whichever is longer. Under OMB guidance, an agency need not keep track of every disclosure at the time it is made, but the agency must be able to reconstruct an accurate and complete accounting of disclosures.

SSA's Disclosure Policy Allows Information Sharing with Law Enforcement under Certain Conditions, but is More Restrictive than the Privacy Act

While SSA's policy permits the sharing of nontax information with law enforcement, it does so only under certain conditions and is more restrictive than both the law enforcement exception specified under the Privacy Act and the disclosure policies of most federal agencies. Before allowing the disclosure of information, SSA's disclosure policy requires SSA officials to consider several factors such as the nature of the alleged criminal activity, what information has been requested, and which agency has made the request. Such considerations are above and beyond what is included in the law enforcement exception to the Privacy Act. SSA maintains that it must have a restrictive disclosure policy because much of the information the agency collects is especially personal. In addition, SSA officials believe that the agency must uphold the pledge it made to the public to keep this information confidential when SSA first began collecting it. Unlike SSA, the policies of most major federal agencies allow the disclosure of information to law enforcement if the requests for

[6]Under implementing OMB guidance, disclosures may also be made to state and local government law enforcement agencies, as well as to federal agencies. "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," Office of Management and Budget, 40 FR 28948, 28955 (July 9, 1975). OMB found support for its guidance regarding law enforcement disclosures in congressional floor statements made regarding the Privacy Act legislation.

information meet the requirements outlined in the Privacy Act. However, like SSA's disclosure policy, the disclosure policies of the IRS and the Bureau of the Census, which have disclosure requirements prescribed in their statutes, are more restrictive than the Privacy Act and the disclosure policies of most federal agencies.

SSA Discloses Information to Law Enforcement under Certain Conditions

While SSA has a long history of protecting individuals' privacy, the agency's disclosure policy allows the disclosure of information to law enforcement under certain conditions. These conditions require that SSA officials consider several factors before they release individuals' personal information. For example, they must examine the nature of the alleged criminal activity, what information has been requested, and which agency has made the request. SSA will share information if the criminal activity involves one of the following:

- ***Fraud or other criminal activity in Social Security programs.*** SSA will provide information necessary to investigate or prosecute fraud or other criminal activity in Social Security programs.

- ***Nonviolent crimes and criminal activity in other government programs that are similar to Social Security programs.*** SSA may also disclose information to investigate and prosecute fraud and other criminal activity in similar benefit programs, including state welfare/social services programs such as Medicare or Medicaid, unemployment compensation, food stamps, and general assistance and federal entitlement programs administered by the Department of Veterans Affairs, Office of Personnel Management, and the Railroad Retirement Board.[7]

- ***Violent and serious crimes.*** SSA may disclose information when a violent crime has been committed and the individual who is the subject of the information requested has been (1) indicted or convicted of the crime and (2) the penalty for conviction is incarceration for at least 1 year and a day regardless of the sentence imposed. SSA might also disclose information when a person violates parole and the violent crime provisions of the original conviction have been met. SSA defines violent and serious crimes as those characterized by the use of physical force or by the threat of physical force causing actual injury, or coercing the victim

[7]Railroad Retirement benefits are authorized under the Railroad Retirement Act and provide income protection to railroad workers and their families during old age, times of disability, or the death of qualified workers.

to act for fear of suffering serious bodily harm. Such crimes include but are not limited to: murder; rape; kidnapping; armed robbery; burglary of a dwelling; arson; drug trafficking or drug possession with intent to manufacture, import, export, distribute or dispense; hijacking; car-jacking; and terrorism.

- ***Provisions of other federal statutes that require that SSA disclose its records such as in connection with civil or criminal violations involving federal income tax or the location of aliens.*** SSA will disclose information when another federal statute requires disclosure, such as the IRS statute for tax purposes or the Immigration and Naturalization statute for locating aliens.

- ***The jeopardy or potential jeopardy of the security and safety of SSA's clients, personnel, or facilities.*** SSA will disclose information about an individual if that individual is involved in an activity that places the health, safety or security of SSA clients, personnel, or facilities in jeopardy or potential jeopardy. After the disclosure, SSA must send a notice of the disclosure to the individual whose record was disclosed.

SSA's disclosure policy is contained in 20 C.F.R. Part 401 and is promulgated through regulations outlined in its "Program Operations Manual System" (POMS) and Emergency Messages. POMS is the primary tool the field offices use to assist them in making appropriate disclosure decisions when they receive requests from law enforcement agencies. POMS provides detailed guidance and incorporates references to disclosures covered by 25 different statutes, which are located in at least 15 different sections of the POMS. SSA uses Emergency Messages, usually limited to a one-time only emergency situation, to provide implementing guidance in emergency situations. For example, on September 19, 2001, SSA issued an emergency message to field offices instructing them to direct all law enforcement requests related to the terrorists' attacks of September 11, 2001, to SSA's OIG's Office.

SSA's regulations are designed for implementation at all levels of the agency, including SSA's field offices, regions, and headquarters offices. SSA can make disclosures through its headquarters, 1,336 field offices, or 10 regional offices. Disclosures can also be made through SSA's OIG, the law enforcement component of SSA that is responsible for conducting audits and investigations of agency programs and activities. The OIG is authorized to handle disclosures through a memorandum of understanding (MOU) with SSA. The OIG investigations staff conducts and coordinates activity related to fraud, waste, abuse, and mismanagement of SSA

programs and operations. The OIG investigations staff also conducts joint investigations with other federal, state, and local law enforcement agencies. The OIG investigations staff is located in 60 locations that comprise 31 field offices and 10 field divisions.

SSA's OIG is authorized to disclose individuals' personal information to law enforcement agencies as agreed with SSA under a MOU. In July 2000, SSA's OIG and the Commissioner of SSA signed an MOU, which outlines the conditions under which the OIG can disclose to law enforcement agencies certain limited information from SSA's records in cases involving fraud of a Social Security program or misuse of an SSN. Under the MOU, the OIG can disclose whether a given name and SSN match the name and SSN in records at SSA, referred to as SSN verification. The MOU delegates authority to OIG employees at all levels. SSA requires that the OIG ensure that law enforcement requests meet the same requirements outlined in the Privacy Act as well as those outlined in SSA's POMS and other guidance. In addition, law enforcement requests must include the name and SSN to be reviewed and a certification that the individual about whom information is sought is suspected of misusing an SSN or of committing another crime against a Social Security program. Under the MOU, the OIG is permitted to open an investigation and participate in joint investigations with law enforcement officials, if the OIG determines that further investigation is warranted.

SSA requires that the OIG submit an annual report to the Commissioner of SSA, no later than 30 days after the end of the fiscal year. The annual report must reflect the total number of SSN verification requests received and responses made, if the number is different, broken down by OIG field division. SSA also requires that the OIG maintain records from each fiscal year for 1 year. The Commissioner of SSA can revoke the delegation of authority to the OIG described in the MOU at any time by providing a 30-day notice.

While any SSA office can make disclosures, the Privacy Officer within SSA's Office of Disclosure Policy, located in the Office of General Counsel, has overall responsibility for overseeing the agency's implementation of the disclosure policy. Except for requests involving national security issues, which are referred to the Privacy Officer at SSA headquarters and ultimately to the Commissioner of SSA, field locations handle requests for disclosing information because the offices are at the local level where information is frequently needed. Privacy Coordinators are located in the regional offices and are available to assist the field offices on questions about disclosures. The Privacy Coordinators report to the Privacy Officer.

When SSA receives a request from law enforcement agencies, SSA officials must first determine whether the request is valid, that is, in writing on the agency's letterhead, specifies the records being requested, and is signed by an official of the requesting office. SSA field office officials are instructed to rely on their knowledge of local law enforcement agencies to determine whether a request is from the proper person. For valid requests, SSA officials must also determine whether the agency requesting the information has jurisdiction in the particular case. Other specific criteria considered in determining whether SSA will disclose individuals' personal information to law enforcement agencies are outlined in figure 1. Tax information is disclosed consistent with IRC 6103. SSA officials told us that in all cases, the agency's practice is to provide only the minimum amount of information necessary to assist law enforcement.

Figure 1: SSA's Disclosure Policy for Law Enforcement

Requester/reason for request		Personal information SSA discloses
Fraud or other criminal activity in Social Security programs		
SSA OIG	– To investigate fraud or other criminal activity in Social Security programs.	Any information contained in SSA's database, including tax return information.
Secret Service	– To investigate allegations of theft, forgery, or unlawful negotiation (cashing, depositing, or other transaction) of Social Security benefit payment checks.	Any information, including tax return information.
U.S. Attorneys	– To investigate violations of the Social Security Act.	Any information, including tax return information.
Federal Bureau of Investigation (FBI)	– To investigate violations of the Social Security Act.	Any information, including tax return information.
Postal Service	– To investigate allegations of theft, forgery, or unlawful negotiation (cashing, depositing, or other transaction) of Social Security benefit payment checks.	Nontax information.
Federal, state, and local agencies	– To apprehend fleeing felons in receipt of Supplemental Security Income (SSI) benefits.	Only Social Security information-SSN, current address, and photograph (if readily available).
	– To apprehend fleeing felons in receipt of Old Age and Survivors Insurance and Disability Insurance benefits (Title II of the Social Security Act).	No information, unless the individual has been indicted or convicted of a serious crime - see category for violent and serious crimes.
Nonviolent crimes or criminal activity in other similar government benefit programs		
Federal agencies	– To investigate eligibility, payments status, and benefit payments of income and health maintenance programs. (Requester must furnish SSN and name or the name and sufficient information to locate an SSN-SSA will not disclose a name if only the SSN is furnished.)	Nontax information.
FBI	– To investigate welfare fraud in Native American Territories[a] (Requester must furnish SSN and name or the name and sufficient information to locate an SSN-SSA will not disclose a name if only the SSN is furnished.)	Nontax information.
U.S. Attorneys	– To investigate welfare fraud in Native American Territories.[a]	Nontax information.
Secret Service	– To investigate allegations of theft, forgery, or unlawful negotiation of Medicare payment checks.	Any information, including tax return information.

SSA's Disclosure Policy for Law Enforcement (continued)

Requester/reason for request		Personal information SSA discloses
Nonviolent crimes or criminal activity in other similar government benefit programs (cont.)		
Postal Service	– To investigate allegation of theft, forgery, or unlawful negotiation of Medicare payment checks.	Nontax information.
ICE DHS[b]	– To identify and locate aliens (Immigration must certify that persons of inquiries are aliens and not U.S. Citizens.[c])	SSN and nontax return information.
	– To identify and locate of alleged Nazi war criminals.	SSN and nontax information.
	– To identify aliens with earnings posted to nonwork SSNs.	Name, SSN, and address of the alien and name and address of alien's employer.
State and local agencies	– To investigate eligibility, payments status, and benefit payments of welfare programs or health or income maintenance programs.	Nontax return information, which may include benefit data, dates of birth, medical records, health insurance data, SSN verification, addresses, and other relevant records.[d]
	– To investigate eligibility, payments status, and benefit payments of federal grants, e.g., Temporary Assistance for Needy Families, Medicaid, state supplemental security income, unemployment, food stamps, or adult assistance.	Tax return information released only under an automated data exchange agreement under IRS safeguard requirements.
Federal, state, and local agencies	– To investigate crimes of embezzlement and shoplifting.	No information.
SSA	– To find instances of possible violations of other agencies' laws, policy, or regulations.	SSA allows disclosure of other information to other agencies if, the possible violation is covered by the "routine use" provision of the Privacy Act. Officials are advised to use judgment when referring cases to other agencies.[e]
Violent and serious crimes		
Federal, state, or local agency	– To investigate or prosecute violent crimes where the subject person has been *indicted* or *convicted* of the crime and the penalty for conviction is incarceration for at least 1 year and a day.	Nontax information limited to information requested but might include address (if not taken from federal tax returns), SSN verification, and other relevant information to the case.
Federal, state, and local agencies	– To investigate parole violations.	Nontax information if the violent crime provisions are met for the original conviction.
	– To investigate individuals **suspected** of a non-Social Security-related crime.	No information.

SSA's Disclosure Policy for Law Enforcement (continued)

Requester/reason for request		Personal information SSA discloses
Violent and serious crimes (cont.)		
Any agency	– To investigate threat against high government officials, such as the President of the United States.	Commissioner of SSA makes decision about what information will be disclosed.[f]
	– To investigate possible espionage, high-jacking, hostage taking, and bombing.	Commissioner of SSA makes decision about what information will be disclosed.[f]
SSA	– To find instances in which high government officials' lives are threatened (e.g., the President or others).	SSA Privacy Officer handles and makes any required referrals to appropriate law enforcement officials or as necessary, refers to the Commissioner for decision.
Foreign or international law enforcement agencies	– To investigate any crime.	Privacy Officer makes determination of what to disclose.
Civil or criminal violations involving federal income tax		
IRS	– To investigate violations of federal tax laws, verify Social Security numbers, or verify benefit amounts when required for tax purposes. (IRS must furnish SSN and name or the name and sufficient information to locate an SSN-SSA will not disclose a name if only the SSN is furnished.)	Relevant Social Security information and tax return information.
Activities that jeopardize security and safety of SSA's clients, personnel, or facilities		
SSA	– To investigate threats to any individual.	Nontax information to aid the police or another appropriate party locate, prosecute, or detain individuals who threaten SSA employees.
	– To investigate threats of suicide.	Nontax information to an appropriate mental health clinic, agency, hotline, or other.

Sources: Social Security Administration (data) and copyright © Corel Corp. All rights reserved (icons).

[a]State officials do not have jurisdiction in welfare fraud cases in Native American Territories; therefore, SSA does not disclose information to state officials.

[b]The Bureau of Immigration and Customs Enforcement of the Department of Homeland Security (ICE DHS) was created with the merger of the former Immigration and Naturalization Service (INS) and Customs Service.

[c]SSA has specific procedures for processing Immigration requests for personal information through its field offices and the Immigration District located in Baltimore, Maryland.

[d]State and local agencies may obtain this information from SSA under automated data exchange.

[e]All requests concerning these crimes are processed at SSA headquarters through the Privacy Officer, who refers the cases to the Commissioner for a decision under the Commissioner's ad hoc authority.

[f]SSA advises staff to consider whether the possible violations are of significant value to the other agency and whether excessive use of SSA's resources would be required to help the other agency in its investigation.

For law enforcement requests that do not fit neatly in the categories described or do not meet the specific criteria outlined in SSA's policy, SSA's Commissioner decides whether or not the agency will share the requested information using the Commissioner's ad hoc authority. The Commissioner's ad hoc authority is generally reserved for exceptional cases approved on a case-by-case basis. For example, following the September 11th, 2001, terrorist attacks, the Commissioner's ad hoc authority was invoked to disclose to the FBI and other law enforcement agencies information in SSA's files concerning suspects or other persons who may have had information on the attacks and to help identify and locate victims and members of their families.[8] Certain requirements must be met in order to invoke the Commissioner's ad hoc authority. The request must be deemed appropriate and necessary, SSA's regulations cannot specify what is to be done in the circumstance in question, and no provision of law can specifically prohibit the disclosure. SSA policy prohibits the disclosure of tax return information under the Commissioner's ad hoc authority. SSA officials told us that the Commissioner invokes this authority infrequently and had rendered decisions to disclose information to law enforcement agencies 35 times between April 1981 and October 2002.

SSA's Disclosure Policy for Law Enforcement Is More Restrictive than the Privacy Act

Unlike SSA's disclosure policy, the Privacy Act requires that fewer criteria be met before a disclosure is made. However, SSA officials state that the agency must protect tax information and maintain the pledge of confidentiality that the agency made long before the Privacy Act was enacted. Therefore, SSA's policy imposes additional requirements as a condition for disclosure. Over the years, SSA has modified its disclosure policy to incorporate legislative requirements, but where it had discretion, SSA has continued to focus its policy on protecting individuals' privacy and upholding the pledge of confidentiality.

[8]As noted in figure 1, SSA's policy usually prohibits the disclosure of individuals' personal information to law enforcement agencies when the person whose information is requested is only *suspected* of a crime. However, in this case, the Commissioner made the decision that it was appropriate to give information on individuals suspected of the criminal activity and the families of the victims.

The law enforcement exception of the Privacy Act permits disclosure of individuals' personal information when a law enforcement agency (1) requests the information for an authorized law enforcement activity, (2) makes the request through the agency head, (3) submits the request in writing, and (4) specifies the information requested and the law enforcement activity involved. Under the Privacy Act, a law enforcement agency investigating a person suspected of embezzlement or shoplifting could submit a request to most federal agencies, including SSA, for information seeking or verifying the person's name, SSN, date of birth, last known address, and other data. Most federal agencies would probably provide that information from their records covered by the Privacy Act. However, under SSA's policy, no information would be given to the law enforcement agency because SSA has determined that these are not crimes that warrant any disclosure of individuals' personal information. Additionally, the Privacy Act includes a routine use exception, which allows personal information to be disclosed on the initiative of the custodian agency. To qualify for a routine use, the proposed use of the information must be compatible with the purpose for which the information was obtained. Agencies must publish their routine uses in the Federal Register. SSA relies on the routine use exception to disclose information to law enforcement when fraud or other violations are suspected in SSA's programs and other similar federal income or health maintenance programs.

SSA's Policy Is More Restrictive than the Policies of Most Federal Agencies, with the Exception of IRS and Census

SSA's disclosure policy[9] is more restrictive than the disclosure policies of most major federal agencies, with IRS and the Census Bureau, being exceptions. However, unlike SSA's disclosure policy, the policies of the IRS and Census are specifically provided in statute. Most major federal agencies' policies allow for disclosures to law enforcement agencies under the law enforcement or the routine use exceptions of the Privacy Act.[10]

The law enforcement exception of the Privacy Act permits all federal agencies to disclose personal information to law enforcement agencies upon written request from the law enforcement agency. Twenty of the

[9]SSA's disclosure policy for nontax information is the subject of this report since disclosure of tax information is only permitted by the IRC.

[10]Components of some agencies have a disclosure policy that differs from the disclosure policy of the agency of which they are a part. For example, the Department of Commerce uses the Privacy Act to guide its disclosures, while Census, which is a component of Commerce, has its own statute. Similarly, IRS, which is a component of Treasury, has its own statute.

24 major federal agencies have issued regulations that reference that disclosure authority.[11] In addition, OMB guidance permits agencies to disclose personal information covered by the Privacy Act to law enforcement agencies under the routine use exception of the Privacy Act. The routine use exception permits federal agencies, at their own initiative, to disclose personal information without consent if the use is compatible with the purpose for which the information was collected. OMB guidance permits such a disclosure to a law enforcement agency when a violation of law is suspected, provided that such disclosure has been established in advance as a "routine use" and the misconduct is related to the purposes for which the information is collected and maintained.[12] Fourteen of the 24 major federal agencies have established law enforcement routine use exceptions that are generally applicable to their systems of records. Some agencies alternatively only apply the law enforcement routine use exception to specific systems of records.[13] Accordingly, under the Privacy Act, disclosure of personal information to law enforcement agencies may be permitted, depending on the agency and the circumstances, either by the law enforcement exception or the routine use exception. SSA, however, does not permit such disclosures from SSA program records under either exception. As already discussed, SSA requires considerations above and beyond the requirements in the Privacy Act. (See app. II for a list of federal agencies' rules referencing the Privacy Act law enforcement disclosure authority and those authorizing a general law enforcement routine use exception.)

Although SSA's disclosure policy for law enforcement is restrictive relative to most other federal agencies, IRS and Census also have restrictive disclosure requirements, which are outlined in these agencies' statutes. IRS's disclosures of tax returns and return information are governed by

[11]We identify the major federal agencies as the 24 agencies covered by the Chief Financial Officers' Act of 1990 and 1994 legislation designating SSA as an independent agency requiring a Chief Financial Officer.

[12]40 Fed. Reg. 28948, 28953, and 28955, July 9, 1975.

[13]The 2001 Compilation of Privacy Act Issuances provides examples of specific systems of records to which the law enforcement routine used is applied: for example, Department of Agriculture, Agricultural Marketing Service, Employment History Records for Licensed Nonfederal Employees (USDA/AMS-1); General Services Administration, Employee-related files (GSA/Agency-1); Small Business Administration, Audit Reports (SBA 015); and Department of the Treasury, Treasury Integrated Management Information Systems (Treasury/DO .002). The Privacy Act Issuances are available on-line from the Government Printing Office (www.gpo.gov).

Internal Revenue Code Section 6103, which prohibits disclosures unless specifically authorized in statute. This statutory restriction serves to protect the confidentiality of personal and financial information in IRS's possession and ensure compliance with tax laws. A court order is generally required to open tax returns or other tax information to federal law enforcement officials investigating a federal nontax crime or preparing for a grand jury or other judicial proceeding, without the knowledge or consent of the taxpayer involved. The Attorney General, the Deputy Attorney General, and other Justice Department officials specifically named in the statute, are permitted to seek a court order. To obtain a court order, the requester has to demonstrate that:

- reasonable cause exists to believe that a specific criminal act has been committed and tax return information is or may be relevant to a matter relating to the commission of the criminal act;

- the information being sought will be used exclusively in a federal criminal investigation concerning the criminal act; and cannot be reasonably obtained, under the circumstances, from another source.

Information federal law enforcement obtains from IRS generally cannot be shared with state and local law enforcement. However, the Victims of Terrorism Tax Relief Act of 2001 permits federal law enforcement agencies involved in terrorist investigations/intelligence gathering to redisclose this information to officers and employees of state and local law enforcement who are directly engaged in investigating or analyzing intelligence concerning the terrorist incidents, threats, or activities.

The disclosure authority for Census is spelled out in statute under Title 13 of the United States Code. The Census statute prohibits the disclosure of any individual's Census data other than for use by the Census, making information that the Bureau of the Census collects and maintains immune from the legal process. Unlike IRS, a court order will not permit the Census Bureau to disclose information to law enforcement agencies or any other entities that may request an individual's personal information. Regulations provide that a person's individual census information may not be disclosed to the public for 72 years from the decennial census for which the information was collected and the fine for wrongful disclosure of confidential census information is imprisonment of up to 5 years or a fine

up to $250,000, or both.[14] The statute further restricts the use of individuals' Census data to the Secretary of Commerce, or bureau and agency employees. Additionally, Census data for individuals may only be (1) used for statistical purposes for which it was supplied; (2) published in a manner so that an individual's information cannot be identified; and (3) examined by persons who have been sworn as officers or employees of the Department of Commerce, or the Bureau of the Census. The statute even protects from compulsory disclosure, copies of Census information that an individual may have retained for their own personal use. Accordingly, "no department, bureau, agency, officer, or employee of the government, except the Secretary of Commerce in carrying out the statutory duties of the agency, shall require copies of information an individual may have retained." An individual's personal retained copies of census forms are immune from the legal process and cannot be admitted as evidence in any action, suit, or other judicial or administrative proceeding without the individual's consent.

SSA Views Restrictions as Integral to Carrying Out Its Mission

SSA maintains that it must have a restrictive disclosure policy to protect individuals' personal information, even from law enforcement requests, because much of the information the agency collects is especially personal and was initially obtained under the pledge of confidentiality. SSA officials told us that they try to limit disclosure because the agency has no control over the extent to which information will be safeguarded once disclosed. In addition, Social Security has universal coverage and an individual cannot refuse to be assigned an SSN. The Social Security Act requires that SSA compile wage and employment data for each individual. According to an SSA official, individuals cannot receive Social Security benefits without having an SSN. In SSA's disclosure policy, the agency recognizes that its rules for disclosure are more restrictive than the Privacy Act and cites several reasons why. According to SSA, it seldom has records that are useful to law enforcement agencies and information from tax returns—such as addresses or employment information—cannot be disclosed. Also, SSA contends that its resources should not be diverted for nonprogram purposes. Finally, SSA says that it has a long-standing pledge to the public to maintain the confidentiality of its records.

[14]The decennial census occurs every 10 years, in the years ending in "0," to count the population and housing units for the entire United States.

SSA Has Provided Information to Law Enforcement Officials, but Confusion about the Disclosure Policy May Cause Inconsistent Application

Although SSA's policy supports sharing limited information with law enforcement under certain conditions, we found evidence that some SSA field office staff are confused about the policy that could result in staff applying it inconsistently. Information provided to law enforcement is generally limited to the verification of a name and SSN, though more information may be provided under certain circumstances. Information obtained through our selected site visits and survey results indicated that SSA field offices might have denied law enforcement requests when they could have provided information and instances in which offices might have provided more information than was permitted under SSA's policy. Because SSA is not required to and therefore, does not maintain aggregated data showing what requests were made, whether they were approved, and what information was given to fulfill them, we could not determine the extent to which these inconsistencies occurred.

Information SSA Provided to Law Enforcement Often Limited to Name and SSN Verification

Information provided to law enforcement is routinely limited to the verification of a name and SSN, though more information may be provided under certain circumstances. When law enforcement provides SSA with the name and SSN of an indicted or convicted criminal, SSA can conduct a search on the SSN to determine if it is valid and if it matches the name provided by law enforcement. If the name and the SSN do not match, SSA will not usually identify to whom the SSN actually belongs, though they will tell law enforcement that there was no match. Except to identify and locate illegal aliens, SSA generally will not provide any information if law enforcement only provides an SSN and wants to know to whom it is assigned. Under certain circumstances, such as when SSA's OIG conducts a joint investigation with other law enforcement agencies involving fraud against one of SSA's programs, the OIG is allowed to provide any information available in SSA's data system, short of IRS data.

SSA's Disclosure Policy Confuses Staff and May Not Be Consistently Applied across SSA Field Offices

SSA tries to ensure that its disclosure policy is consistently implemented in all field offices. SSA takes various steps to ensure the consistent applications of its disclosure policy. For example, SSA has taken steps to educate its staff about its disclosure policy. SSA managers indicated that SSA staff is given disclosure policy training when they start employment and such training is refreshed as needed. Additionally, SSA posts the policy on its internal Web site and on Compact Disc-Read-Only Memory (CD-ROM) for staff reference. Furthermore, a regional "privacy coordinator" is available to answer staff questions about proper disclosure procedures. One SSA regional office provided a chart to all SSA field

offices within its "program circle"[15] that briefly summarizes SSA's policy on access and disclosure without consent. Although this chart had not been updated since July 1996, it was viewed by the manager we talked with as a handy guide for what could be disclosed and also provided references to the location of a more thorough explanation of SSA's policy in their POMS. In addition, to ensure that disclosure procedures are followed, field office managers told us that they usually handle information requests from law enforcement officials rather than leaving this duty to staff.

However, we noted in our survey and during selected site visits, a limited number of instances where SSA's disclosure policy appears to have been inconsistently applied. In some instances, law enforcement might have received more information than permitted under SSA's policy. For example, one SSA OIG office we visited provided a law enforcement agency with the name, SSN, date of birth, place of birth, and parents' name when it seemed that only the name and SSN verification results should have been provided. In another case, an SSA official reported that a state law enforcement officer stopped an individual and telephoned SSA requesting information to verify the SSN, date of birth, place of birth, and sex and was provided the results over the telephone. Although SSA's policy permits the verification of the name and SSN, such requests are required to be in writing. In other instances, requests that should have been approved might have been turned down. For example, one SSA field office manager told us that nothing could be disclosed to law enforcement if the request for information pertained to an individual suspected of misusing an SSN because the individual had not been indicted or convicted of this crime. However, SSA's policy would appear to permit disclosure in this situation. Another SSA field office manager told us that office would not disclose any information without consent from the individual for whom the information is being requested.

Several possible reasons exist for the inconsistent application of SSA's disclosure policy. Although our survey showed that most SSA field offices receive requests for information from law enforcement, SSA field officials we spoke with said that they do not receive requests frequently. For example, several officials told us that they received fewer than 10 requests in 2002. Because requests are infrequent, staff must often consult the policy to help them to respond properly. However, many staff members

[15]The "program circle" consisted of 12 SSA field offices within the area of this particular regional office.

consider the policy confusing. For example, one field office manager said that, "We have doubts as to what information should be provided to U.S. Border Patrol." Similarly, a manager in another field office said, "SSA['s] disclosure policy should be written in "Plain English" to make it easy to understand by all readers." A different field office manager commented, "[SSA's] Disclosure policy is still frequently confusing for much of our staff." This lack of clarity leads to confusion about what should be disclosed. For example, one manager said, "[SSA's policy] is quite confusing. It's hard to know what you can disclose." Another manager commented, "I think the policy should be clearer than it is. There's too much…'if this, then that, but not this and so on.'"

In addition, SSA's responsibilities to both assist law enforcement and protect individuals' privacy may be exacerbating the confusion and inconsistent application of the agency's policy. For example, officials at SSA headquarters said that they want to help law enforcement as much as possible, but they believed they must also protect the privacy of the information in their systems of records in order to perform SSA's primary mission. Some managers in SSA field offices believed that the agency should provide information to law enforcement. However, several field office managers expressed their concerns and reluctance about sharing information with law enforcement agencies. Employees who provide information to an individual inappropriately could be subject to a penalty, including suspension or termination from SSA. Therefore, rather than risk disclosing information inappropriately, some officials might err on the side of caution and not disclose information even when it is permitted under the agency's disclosure policy.

SSA Field Offices Do Not Maintain Aggregated Data, but OIG Does

Consistent application of SSA's disclosure policy cannot be assessed because, according to OMB guidelines, SSA is not required to maintain aggregated data showing what requests were made, whether they were approved, and what information was given to fulfill them.[16] According to SSA, disclosures of individuals' personal information are kept in individuals' files. While SSA policy does not stipulate that field offices must keep track of requests made by a law enforcement agency, our survey revealed some information about these requests. For example, we estimate that 82 percent of SSA field offices indicated that they had

[16]OMB guidance requires that agencies be able to reconstruct an accurate and complete accounting of disclosures. However, we did not request that SSA reconstruct the accounting of disclosures to law enforcement agencies because it was beyond the scope of this assignment, and according to SSA, such a request would involve a huge undertaking.

received requests for personal information from law enforcement agencies. However, 71 percent of SSA's field offices do not maintain a record of requests made by law enforcement agencies.

While the majority of SSA field offices do not maintain records of law enforcement requests, results from our survey showed that 90 percent of the SSA OIG offices maintain these data for disclosures the OIG made. The SSA OIG is required to report to the SSA Commissioner aggregated data annually on disclosures made. According to the OIG, it also keeps a hard copy of requests made by law enforcement agencies for at least 1 year. On the basis of these aggregated data, between fiscal years 2000 and 2002, SSA OIG regional divisions fulfilled almost 30,000 requests from law enforcement agencies for name and SSN verification. Table 2 shows the number of verifications fulfilled by SSA OIG regional divisions and headquarters. However, no numbers are kept on denied law enforcement requests. According to SSA OIG officials, in most cases, law enforcement officers contact OIG offices by telephone before submitting a request so no written record exists if the OIG does not grant the request for information.

Table 2: Number of Information Requests Granted to Law Enforcement by OIG Field Divisions and Headquarters in Fiscal Years 2000 through 2002

Field divisions and headquarters	Fiscal year 2000	Fiscal year 2001	Fiscal year 2002	Total
Atlanta	D – NC[a]	198	1,660	1,858
Boston	D – NC	391	1,072	1,463
New York	52	307	2,202	2,561
Philadelphia	D – NC	405	1,748	2,153
Chicago	D – NC	2,872	7,289	10,161
Dallas	320	439	1,767	2,526
St. Louis	237	894	1,467	2,598
Denver	176	173	1,184	1,533
Los Angeles	400	553	2,353	3,306
Seattle	D – NC	520	282	802
Headquarters	—	—	838	838
Totals	**1,185**	**6,752**	**21,862**	**29,799**

Source: SSA OIG data.

[a]D – NC – Records destroyed; no counts available. Prior to fiscal year 2000, law enforcement verifications were conducted by Allegation Management Division (OIG Hotline), and records no longer exist for those verifications. In April 2002, the Office of Investigations began using the code "LEVER" when conducting law enforcement verifications in the SSA system. The use of "LEVER" will provide OIG with an automated retrieval of the count, and manual counts will no longer be used effective fiscal year 2003.

While Some Law Enforcement Officers Were Unfamiliar with the Policy, Most Were Generally Satisfied with the Information Shared

While some law enforcement officials we spoke with were unfamiliar with SSA's disclosure policies, most were generally satisfied with the information provided by SSA, though most would like more. Some law enforcement agencies at the state and local level were unfamiliar with the process for obtaining information and expressed frustration with their attempts to obtain information from SSA. Law enforcement officials indicated that the SSN and name verification SSA provided was often helpful to their investigations. However, most wanted SSA to provide additional information such as address, date of birth, and employer or family information. SSA officials have several concerns about expanding SSA's disclosure policy.

Many State and Local Law Enforcement Officers Were Unfamiliar with SSA's Disclosure Policy and Procedures

Findings from site visits indicated that some law enforcement officers at the state and local level, who generally request information from SSA field offices, are unfamiliar with the process for obtaining information from SSA offices. Because SSA does not have written procedures on its disclosure policy available to law enforcement, some officers find out how

to obtain information virtually by trial and error. For example, one officer told us that after having his initial request for information, which was not in writing turned down because he had not followed proper procedures, he obtained a search warrant to obtain the information from SSA. The officer said that no one at SSA explained to him the procedures for obtaining information until he got the search warrant. It is unclear when or if SSA officials let law enforcement officers know what procedures need to be followed to get information. Federal law enforcement agencies, on the other hand, more often understood the Privacy Act's procedures. Further, most federal law enforcement agencies we spoke with submitted their requests to SSA's OIG—itself, a federal law enforcement agency. Our survey results indicated that on average in 2002, 46 percent of the requests made to OIG offices came from federal law enforcement agencies while 27 percent of the requests made to SSA field offices on average came from federal law enforcement agencies.

While details on SSA's disclosure policy are available in their POMS and other SSA documents that summarize this information, it is not readily available to law enforcement. A summary of the policy can be found on SSA's Web site under the caption "Code of Federal Regulations for Social Security." However, it is not easy to find and provides little detail on what SSA will provide to law enforcement. Further, the Web site does not provide law enforcement with instructions on what they need to do to get the information.

Most Law Enforcement Officials Found Shared Information Useful but Many Believed More Information Was Needed

Officials from federal, state, and local law enforcement agencies we spoke with were generally satisfied with the information provided by SSA although most would like more information on individuals. Law enforcement officials indicated that, although in most cases SSA only verified a name and SSN, the information received was useful to their investigations and, in some cases, was enough to help convict an individual of a crime. The information received from SSA was considered by law enforcement as the most accurate and up-to-date information available to help in their investigations.

Law enforcement was also satisfied with the time in which SSA provided the information. In many cases, law enforcement officers we spoke with indicated that SSA provided the information very quickly. In addition, one SSA OIG official told us that when procedures are followed correctly, the OIG can reply back in 24 hours or less, depending on the information requested. SSA confirmed the timeliness of its responses to law enforcement requests. We estimate that over 90 percent of both SSA field office and OIG respondents reported that it took 24 hours or less to fulfill a

request. Our survey results showed that 40 percent of SSA field offices and 21 percent of SSA OIG offices reported that it took less than an hour to fulfill a request from a law enforcement agency.

Although most of the law enforcement officials we spoke with were satisfied with information provided by SSA, several believed the information provided was insufficient. Several of these law enforcement officials believed that the name and SSN verification was not enough to help with their investigations. These individuals generally wanted additional information such as the suspect's wage information, address, employer, and date of birth. In documents provided to us, SSA's OIG listed the following situations in which the OIG could not provide information to law enforcement.

When the official

- provides the SSN and wants to know to whom it is assigned;
- wants information to locate witnesses or suspects in high profile cases or missing persons;
- wants information on individuals with Alzheimer's disease who are lost,
- wants information on next of kin;
- wants information to locate a fugitive who may be receiving benefits under SSA's Old-Age and Survivors Insurance program and its Disability Insurance program;
- wants information to make identifications in child pornography cases;
- wants information to determine if there has been any activity on a Social Security account in a custodial interference case;[17] and
- wants information on SSNs related to non-SSA-related fraud cases or counterfeit cases.

[17]A custodial interference case usually involves the actions of one spouse who kidnaps a child from the spouse who has custody of the child. The Social Security account can provide information that could help to locate the spouse who kidnapped the child.

Some law enforcement officials were unhappy with SSA's refusal to provide such information, especially because they believed that SSA could easily provide it in a short period of time. For example, one federal officer who investigates nonviolent felony crimes said that SSA seems more concerned about someone committing fraud against one of its programs than about identity theft involving the use of someone's SSN. He also said that SSA would not provide him with any information on the person whose identity was being stolen. Another officer said that because he could not get necessary information from SSA, he had resorted to other means of gathering the information needed. The officer said that depending on resources available, it could take up to 3 weeks to get someone's SSN through other sources. Furthermore, the officer said that while he could make the case without the SSA information, the information SSA can provide would be invaluable to helping fully prosecute a case.

Many SSA officials in the field and OIG offices agreed that SSA's disclosure policy is too restrictive. Many believed that, for legitimate investigations, the policy should allow for disclosures to law enforcement officials of whatever information they need. One SSA OIG official said that, as a law enforcement officer, he believed that he should be able to provide information to another law enforcement officer especially when he knew that doing so would help with a case and also because law enforcement officers would be more willing to share information with the OIG. While the SSA Commissioner can invoke ad hoc authority for certain specific cases to disclose information, as was done in response to the disclosure requests related to the September 11 terrorist attacks, SSA officials said that the use of this authority must be limited. SSA headquarters officials believe that expanding its disclosure policy would hamper its ability to ensure that individuals' personal information is protected and that resources are not diverted from administering Social Security benefit programs.

Conclusions

Protecting individuals' privacy and providing information to law enforcement that could be helpful in solving crimes or ensuring national security are two important yet sometimes seemingly conflicting policy objectives. SSA places a high priority on privacy, and its policy for disclosure to law enforcement agencies goes beyond the requirements of the Privacy Act. SSA's disclosure policy attempts to preserve its pledge to maintain individuals' privacy while cooperating with law enforcement and complying with applicable statutes. The end result is a complex policy that is more restrictive than the Privacy Act requirements and those of most federal agencies and more like the policies of IRS and Census, agencies

that maintain personal information whose requirements are embodied in statute.

In addition, some SSA field office staff and local law enforcement officers find SSA's policy confusing and sometimes frustrating. As a possible consequence of SSA staff and local law enforcement's confusion about SSA's policy, law enforcement may be denied requested information even though SSA's policy permits its disclosure or law enforcement may receive information that SSA's policy does not permit. Although we could not assess the overall level of consistency in the application of SSA's policy, we believe eliminating or reducing confusion about the agency's policy would help ensure consistent application, and that this can be achieved with relatively modest actions on SSA's part.

Recommendations

To help ensure consistent application of SSA's disclosure policy for law enforcement in all of its offices and to better assist law enforcement agencies making disclosure requests, we recommend that the Commissioner of SSA do the following:

- Take steps to eliminate confusion about the agency's disclosure policy. These steps could include clarifying SSA's policy; providing additional or refresher training to staff; or delegating decision-making authority for law enforcement requests to specified locations such as the OIG, regional privacy coordinators, or other units that SSA determines would have expertise in this area.

- Provide law enforcement with information on SSA's disclosure policy and procedures. For example, this information could be provided on its Web site, in informational pamphlets, or some other written format.

Agency Comments and Our Evaluation

We obtained written comments on a draft of this report from the Commissioner of SSA. SSA's comments are reproduced in appendix III. SSA also provided technical comments, which we incorporated in the report as appropriate. We also provided a draft of this report to the Departments of Commerce, Justice, and Treasury for review and comment. These three agencies reported that they had no comments.

SSA stated that our draft report accurately reflected the importance of SSA's disclosure policy to the agency's mission but it presents an incomplete description of both the statutory basis for and rationale behind the policy. Further, SSA stated that the draft report does not take into

account the statutory basis for the nondisclosure of tax information or the statutory support for the agency's long-standing confidentiality pledge; therefore, SSA believes that our findings and recommendations are "overbroad." We are aware of SSA's obligation under the IRC and took this into consideration during our review of SSA's disclosure policy; however, we have revised the report, where appropriate, to clarify that our observations about SSA's disclosure policy relative to the Privacy Act do not extend to SSA's disclosure of tax information. Disclosure of tax information is controlled by section 6103 of the IRC. We also provided additional reference to the statutory basis and rationale behind SSA's disclosure policy.

SSA also commented that 42 U.S.C. 1306 provided an independent basis for nondisclosures, apart from the Privacy Act. The report recognizes that 42 U.S.C. 1306 provides the basis for SSA's disclosure policy and we have added a citation for this authority. Section 1306 provides SSA authority to regulate the dissemination of information in its custody as otherwise permitted by federal law. Other federal law includes the Privacy Act. Our report merely points out that SSA has used this authority to regulate in a more restrictive fashion than the Privacy Act requires.

SSA stated that it believed that our characterizing the agency's policy as more restrictive than most federal agencies does SSA a disservice because many federal agencies have little interaction with the public at large. SSA states that the only two agencies of SSA's size and scope with respect to gathering information from the public to accomplish their missions are IRS and Census, which have more restrictive disclosure policies and statutes that prohibit disclosures. We believe that our comparison and characterization of SSA's disclosure policy is fair. We compared SSA's disclosure policy to those of the other 23 agencies covered by the Chief Financial Officers' Act. We decided also to compare SSA's policy to those of IRS and Census because they are similar in size and scope of data maintained on individuals. All of the agencies we compared are subject to the Privacy Act. As we reported, SSA's disclosure policy, as well as those of IRS and the Census Bureau is more restrictive than most federal agencies.

SSA agreed in part with our recommendation that the Commissioner take steps to eliminate confusion that may cause inconsistent application of the policy. SSA acknowledged that the policy is complex and could lead to occasional inconsistent application. However, SSA stated that it provides extensive instructions in its POMS for employees and the instructions refer staff to experts in regional and central offices for assistance when

needed. SSA also stated that its regional offices have provided employees access to Intranet sites that clarify disclosure policy, but the agency will consider providing additional refresher training as appropriate. In addition, SSA stated it is currently reviewing improvements to the POMS sections that address law enforcement disclosures that the agency believes will address our concerns. SSA expressed concern about the option to consider delegating "decision-making authority for law enforcement requests to specified locations such as the OIG..." SSA stated that the Inspectors General Act of 1978 prohibits agencies from transferring programmatic functions to the Inspector General.

We acknowledge in our report that SSA provides guidance on its disclosure policy in its POMS. While we found that employees were aware of this guidance, SSA staff told us that they found SSA's policy confusing. We believe additional training as well as improvements to the POMS that clarify or simplify SSA's policy should help ensure consistent application.

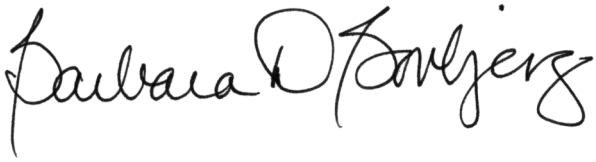
With respect to SSA's concern about our recommendation to consider delegating decision-making authority for law enforcement requests to specified locations such as the OIG, regional privacy officers, or other units that SSA determines would have expertise in this area, we did not intend to imply that programmatic functions be transferred to the OIG. Our recommendation was aimed at directing disclosure requests to units that currently perform this function and that appear to have expertise in SSA's disclosure policy. We simply intended to provide options for SSA to better utilize the resources they already have in place to determine whether law enforcement requests are permitted under SSA's disclosure policy. The OIG, who currently responds to law enforcement requests as authorized under an MOU with SSA, was only one of the units we suggested as an option. We continue to believe that delegating authority to handle disclosure requests to specified units with expertise in SSA's disclosure policy would be a plausible option for helping to ensure consistent application of SSA's policy. This option could reduce or eliminate the need for SSA field office officials who receive sporadic requests from law enforcement to relearn SSA's disclosure policy.

SSA agreed with our recommendation that the Commissioner of SSA should provide law enforcement with information on SSA's disclosure policy and procedures and SSA believes the agency has done so. However, SSA stated it would review its Web site and other public informational materials to see if additional material or formatting changes would be helpful.

We acknowledged in our report that SSA's policy can be found on the Internet, but noted that it is not easily found and does not clearly explain how law enforcement could obtain information. Although SSA officials told us that they provided limited discussion of the agency's disclosure policy and procedures at law enforcement conferences, these officials did not indicate the number of conferences attended or whether these conferences involved federal, state, or local law enforcement. Some of the local law enforcement officials we spoke with were unfamiliar with how to obtain information from SSA. Therefore, we continue to believe that information that clearly defines SSA's disclosure policy and procedures would be helpful to law enforcement. Further, we believe that our findings and recommendations are central to many concerns expressed by both SSA and law enforcement officials and we view the steps that SSA indicated that it plans to consider, or already has in process to ensure consistent application of its disclosure policy and law enforcement's understanding of how to obtain information from SSA as appropriate steps toward correcting the concerns expressed.

We are sending copies of this report to the Commissioner of Social Security; the Secretaries of Commerce, Treasury, and Homeland Security; the U.S. Attorney General; appropriate congressional committees; and other interested parties. We will also make copies of this report available to others on request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staffs have questions about this report, please call me on (202) 512-7215. Other GAO contacts and staff acknowledgments are listed in appendix IV.



Barbara D. Bovbjerg
Director, Education, Workforce,
and Income Security Issues

Appendix I: Scope and Methodology

To attain our objectives for this assignment, we reviewed and compared the Social Security Administration's (SSA) disclosure policy for law enforcement and the Privacy Act. We also compared SSA's disclosure policy with that of the Internal Revenue Service (IRS) and the Bureau of the Census because SSA officials believe that these agencies are comparable with SSA. Additionally, we compared SSA's disclosure policy with the general law enforcement disclosure policies for the other 23 Chief Financial Officers' (CFO) Act agencies.

To help determine how SSA's disclosure policy affects information sharing with law enforcement, we conducted site visits and detailed interviews at SSA field offices and SSA's Office of the Inspector General (OIG), as well as nearby field offices for federal, state, and local law enforcement agencies in Los Angeles, California; Chicago, Illinois; and Dallas, Texas. We also administered an electronic survey to all SSA OIG field offices[1] and a stratified random sample of SSA field offices.

We interviewed SSA officials in both headquarters and field offices and law enforcement officials at the federal, state, and local levels of government about their experiences with sharing individuals' personal information. At the headquarters level, we interviewed SSA officials responsible for disclosure policy in the Office of General Counsel and the SSA OIG, Baltimore, Maryland. We interviewed law enforcement officials from the Departments of Justice and Treasury, including the Federal Bureau of Investigation (FBI); Bureau of Immigration and Customs Enforcement, formerly Immigration and Naturalization Service (INS) and Customs; Executive Office for United States' Attorneys; Drug Enforcement Agency; United States Marshals Service; Secret Service; Internal Revenue Service (IRS); and Alcohol, Tobacco and Fire Arms, headquartered in Washington, D.C. During the course of our review, several of these law enforcement agencies merged into the Department of Homeland Security, or were otherwise reorganized.[2] We also interviewed OIG officials for investigation at the Departments of Education and Housing and Urban

[1]SSA OIG officials identified 31 field offices of its 60 locations as the universe of field offices to survey. According to the officials, the remaining locations are satellite offices that report to the 31 offices identified.

[2]Effective January 2003, the Bureau of Alcohol, Tobacco and Firearms reorganized with the law enforcement functions transferred to the Department of Justice, but the tax and trade functions remained in the Department of the Treasury. Effective March 2003, the Secret Service, Customs, and Immigration and Naturalization Service were merged into the newly created Department of Homeland Security.

Development in Washington, D.C. Our site visits included interviews with the Bureau of Immigration and Customs Enforcement, at Dallas, Texas, and law enforcement officials of the Arlington Police Department, Arlington, Virginia.

We surveyed SSA offices in order to: (1) estimate the type and volume of law enforcement requests for personal information received by SSA; (2) determine the distribution of these requests across federal, state, and local law enforcement agencies; and (3) gain some understanding of the bases for the granting and denial of these requests. Our working definition of a personal information request is an instance for which a law enforcement agency requested the personal information of one or more individuals between fiscal years 1999 and 2002. For example, if a law enforcement agency requested addresses for two people in a single instance, this would count as one personal information request. We were specifically interested in law enforcement agencies' requests for personal information, such as social security numbers, names, addresses, birth dates, and income.

We designed an Internet-based survey and organized it into multiple sections that included the following areas: receipt of law enforcement requests, response time for fulfilling law enforcement requests, and methods for handling law enforcement requests. We selected a stratified random sample of 335 SSA field offices to participate in the survey. This number was based on an expected response rate as well as a precision level. The sample was stratified by 10 regional locations and taken from a listing of 1,286 field offices that SSA provided. The original list contained 1,336 locations. Fifty locations that are not considered field offices and, therefore, do not receive law enforcement agency requests were excluded from the sampling frame. All 31 SSA Inspector General offices were surveyed since these sites routinely accept law enforcement agencies' requests for personal information. The survey was mailed electronically to the manager in charge at SSA and Inspector General field offices. Both office types received the same on-line survey. Survey data were collected between February 25, 2003, and March 21, 2003. The overall response rate was 90 percent; with 97 percent of the Inspector General's field offices and 90 percent of SSA's field offices responding. Regional response rates in the sample ranged from 86 percent to 95 percent across 10 regional locations.

To provide some indication of the reliability of the survey results, standard errors were calculated. The sample was weighted in the analysis to statistically account for the sample design and nonresponse. We are 95 percent certain that the survey estimates provided in this report are

within plus or minus 10 percentage points of those estimates that would have been obtained had all SSA offices been captured.

To minimize some of the potential biases of other errors that could figure into the survey results, we conducted pretests that included both the SSA Inspector General and SSA field offices. Four pretest sites were SSA field offices located in Wheaton, Maryland; Washington, D.C. (Anacostia); Seattle, Washington; and Chicago, Illinois. One pretest site was an SSA Inspector General office located in Washington, D.C. The pretests were conducted either through teleconferences or face-to-face interviews, and were completed between December 2002 and January 2003.

We conducted our audit work between August 2002 and July 2003 in accordance with generally accepted government auditing standards.

Appendix II: Chief Financial Officers' Act Agencies' Rules on Disclosure of Records to Law Enforcement

Federal agencies	Rule referencing Privacy Act disclosure authority	General routine use exception of Privacy Act permits disclosure to law enforcement[a]
Agriculture	7 CFR 1.119	
Commerce	15 CFR 4.30(a)(5)(vii)	46 FR 63501 (12/31/81)
Defense	32 CFR 310.41	32 CFR 310 App. C
Education	34 CFR 5b.9(b)(7)	34 CFR 5b. App. B
Energy	10 CFR 1008.17(b)(7)	
Health and Human Services	45 CFR 5b.9(b)(7)	45 CFR 5b. App. B
Housing and Urban Development	24 CFR 16.11(a)(5)	2001 Privacy Act Issuance
Interior	43 CFR 2.56(b)(5)	
Justice		
Labor		67 FR 16816 (4/8/02)
State		2001 Privacy Act Issuance
Transportation	49 CFR 10.35(a)(7)	2001 Privacy Act Issuance
Treasury	31 CFR 1.24(a)(7)	
Veterans Affairs	38 CFR 1.576(b)(7)	
Environmental Protection Agency	40 CFR 16.10	67 FR 8246 (2/22/02)
National Aeronautics and Space Administration	14 CFR 1212.203(f)(7)	2001 Privacy Act Issuance
Agency for International Development	22 CFR 215.10(c)(7)	2001 Privacy Act Issuance
Federal Emergency Management Agency	44 CFR 6.20(g)	67 FR 3193 (1/23/02)
General Services Administration	41 CFR 105-64.201(g)	
National Science Foundation		
Nuclear Regulatory Commission	10 CFR 9.80(a)(7)	67 FR 63774 (10/15/02)
Office of Personnel Management	5 CFR 293.401(g) & 406	60 FR 63075 (12/8/95)
Small Business Administration	13 CFR 102.22(h)	
Social Security Administration	20 CFR 401.110 plus more stringent requirements	

Source: GAO analysis, Office of General Counsel data.

[a]Agencies may also have provisions for routine use disclosures for law enforcement for specific systems of records. The 2001 Compilation of Privacy Act Issuances provides examples of specific systems of records to which the law enforcement routine used is applied: for example, Department of Agriculture, Agricultural Marketing Service, Employment History Records for Licensed Nonfederal Employees (USDA/AMS-1); General Services Administration, Employee-related files (GSA/Agency-1); Small Business Administration, Audit Reports (SBA 015); and Department of the Treasury, Treasury Integrated Management Information Systems (Treasury/DO .002). The Privacy Act Issuances are available on-line from the Government Printing Office (www.gpo.gov).

Appendix III: Comments from the Social Security Administration

SOCIAL SECURITY
The Commissioner

August 29, 2003

Ms. Barbara D. Bovbjerg
Director, Education, Workforce
and Income Security Issues
U.S. General Accounting Office
Washington, D.C. 20548

Dear Ms. Bovbjerg:

Thank you for the opportunity to review and comment on the draft report "The Social Security Administration's (SSA) Disclosure Policy for Law Enforcement Allows Information Sharing, But SSA Needs to Ensure Consistent Application" (GAO-03-919). Our comments on the report are enclosed.

If you have any questions, please have your staff contact Laura Bell at (410) 965-2636.

Sincerely,

Jo Anne B. Barnhart

Jo Anne B. Barnhart

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235-0001

COMMENTS ON THE GENERAL ACCOUNTING OFFICE (GAO) DRAFT REPORT "THE SOCIAL SECURITY ADMINISTRATION'S (SSA) DISCLOSURE POLICY FOR LAW ENFORCEMENT ALLOWS INFORMATION SHARING, BUT SSA NEEDS TO ENSURE CONSISTENT APPLICATION" (GAO-03-919)

Thank you for the opportunity to review and comment on the draft report. We are concerned that the draft report presents an incomplete description of both the statutory basis for and the rationale behind our disclosure policy. Because the draft report does not take into account either SSA's statutory authority or its obligations under the Internal Revenue Code (IRC), we believe that GAO's findings and recommendations are over-broad. In addition, we are providing relevant information on our policy that we think should also be included in the draft report because it affects the GAO conclusions that suggest that our disclosure policy is too restrictive, confusing, and that we could cooperate with law enforcement more.

General Comments

The report accurately reflects that SSA considers its disclosure policy to be an integral part of the Agency's mission. Our mission is to "advance the economic security of the nation's people through compassionate and vigilant leadership in shaping and managing America's social security programs." To ensure proper service delivery to the public and to enhance program stewardship, we must have access to a great deal of personal information, including medical, earnings, identity, and employment information. Given the very personal nature of the information, it is imperative that members of the public trust that we will maintain and use it in a private and secure manner. We have always stressed the importance of protecting the privacy of such information; we demonstrated our commitment to protect the privacy of such information as early as 1937 when we issued our first regulation concerning the privacy of information. It has been our experience that the general population provides us with accurate and timely records, knowing that their information will be safeguarded as promised.

Our responsibility to protect individuals' personal information provides a natural tension with our commitment to be responsive to law enforcement as we seek to balance those sometimes competing interests. However, we are concerned that the report gives the impression that SSA is not cooperative with law enforcement agencies. This may have been unintentional, as the table in the report clearly shows multiple examples of cooperation between SSA and the law enforcement community. We have included some additional examples of cooperation below that were not included in the draft report.

We believe that characterizing our policy as more restrictive than "most Federal Agencies," many of which have little interaction with the public at large, does SSA a disservice. We believe the report should be presented in the context of how dependent our mission is on being able to safeguard the personal information given to us on a daily basis. In other words, SSA should be compared only to organizations whose operations

are equally dependent on private data. Other agencies, whose missions may not rely on safeguarding the personal information in their records or may not maintain much personal information at all, may not need to protect information to the same degree as SSA. To compare agencies that have little interaction with the public at large with an agency like SSA that interacts with nearly every person at some point in his or her life is not a fair or useful comparison.

The only two agencies of SSA's size and scope with respect to gathering information from the public to accomplish their missions -- the Internal Revenue Service (IRS) and the Bureau of the Census -- are more restrictive in their disclosure policies, and have statutes that prohibit disclosure. SSA has an independent statutory basis for its disclosure policy, a basis which the report does not acknowledge. In addition to the Privacy Act, SSA records are protected by section 1106 of the Social Security Act. *See* 42 U.S.C. 1306. This statute prohibits the release of any information obtained by any employee of the Social Security Administration at any time, except as permitted by the Commissioner's regulations and as otherwise permitted by federal law. *Id.* Because of the highly sensitive data kept by the Agency in its systems of records, Congress has granted the Commissioner additional authority in statute, aside from that granted by the Privacy Act, to determine whether such discretionary disclosures are appropriate.

Under section 1106, if a disclosure is not permitted under the Commissioner's regulations, there are far more serious consequences for the individual responsible for the disclosure than would be possible under the Privacy Act. Specifically, under the Privacy Act, if an employee improperly releases information, the individual whose records were disclosed may bring a civil action against the agency for injunctive relief and damages. 5 U.S.C. 552a(g). Damages will only be awarded, however, if the agency acted willfully or intentionally. Similarly, the Privacy Act's criminal penalties only apply if the employee acted willfully. 5 U.S.C. 552a(i). However, under section 1106, the Social Security Act has a far lower threshold, as <u>any person</u> who unlawfully discloses information protected by section 1106 (which is all information possessed by SSA), regardless of intent, is guilty of a felony, and may be fined up to $10,000, sent to prison for up to 5 years, or both.

Moreover, the report overlooks our ownership of and accountability for information that falls under the Internal Revenue Code (IRC). A great deal of data in our possession is considered tax return information, and subject to the strict limitations on disclosure contained in the IRC. *See* 26 U.S.C. 6103. Specifically, we obtain tax return information to help administer our programs and to cooperate with IRS in combined annual wage reporting. *See* 26 U.S.C. 6103(l). The IRC clearly states that no one may disclose tax return information except as permitted in that section. *See* 26 U.S.C. 6103(a). SSA works closely with the IRS on disclosures of tax return information, especially in the law enforcement context. Like the IRS, however, SSA must comply with the provisions of the IRC that limit disclosure in the law enforcement context. *See* 26 U.S.C. 6103(i). In several parts of the report, GAO states that SSA does not disclose employer, wage, earnings, and address information to law enforcement, and that law enforcement would like this information. In most cases, however, disclosing this information would be a

violation of the requirements of the IRC, and subject the employee to felony criminal sanctions and immediate dismissal as outlined in the IRC. *See* 26 U.S.C. 7213, 7213A.

The report does not explain that we often must deny requests because requesters are seeking tax return information, and that the disclosure of tax return information in the manner described is prohibited by law. *See* 26 U.S.C. 6103. To the extent that GAO attributes such denials to SSA's policy discretion, the report is fundamentally flawed. We believe it would be more consistent with the stated purpose of the report to consider only those requests that were not seeking tax return information and thus were made exclusively under the SSA regulatory scheme. Similarly, GAO should compare SSA to other agencies that use and possess tax return information to determine whether SSA's disclosure policy with respect to disclosure of tax return information is consistent with those agencies' policies. Some of these agencies include the Departments of Veterans Affairs, Health and Human Services, Labor, Treasury, Commerce, and Justice. Finally, we are concerned that the report contains several statements and recommendations based not on survey findings, but on statements from individuals and on anecdotal findings. Specifically, the report cites "a limited number of instances where SSA's disclosure policy appears to have been inconsistently applied" which is the basis for recommendation number one, while GAO's survey data indicates a general satisfaction and understanding of the policy. For this reason, GAO's conclusions are not supported by the text of the report.[1]

Our responses to the specific recommendations are provided below and we have included technical comments that should be made to enhance the accuracy of the report.

Recommendation 1

The Commissioner of SSA should take steps to eliminate confusion about the Agency's disclosure policy.

Comment

We are pleased that the report acknowledges that, with few cited exceptions, SSA employees follow appropriate disclosure policies and that the law enforcement community generally understands and is satisfied with the information shared.

Regarding the conclusion that the policy is confusing and that it may not be consistently applied, we agree in part. While we acknowledge that the policy is somewhat complex, we provide extensive instructions in our Program Operations Manual System (POMS) for all employees. These instructions are also available to the public and law enforcement authorities. We recognize that some offices do not deal with law enforcement disclosures

[1] Our privacy practices were also referenced as a good example by GAO in the July 2003 report titled "Privacy Act: Office of Management and Budget Leadership Needed to Improve Agency Compliance" (GAO-03-304). That report examined the application of the Privacy Act in 25 Federal agencies. During our interaction with OMB on that report, GAO staff complimented us on the thoroughness of our privacy policies and asked for our advice on several issues such as "routine uses" and "systems of records."

on a regular basis, which may lead to occasional inconsistent application. However, our instructions refer staff to experts in regional and central offices for assistance when needed.

With respect to the additional steps GAO identified that include clarifying the policy and providing additional or refresher training to staff, our regional offices have provided employees access to Intranet sites that clarify disclosure policy. We will consider providing additional refresher training as appropriate. In addition, we are currently reviewing improvements to the POMS sections that address law enforcement disclosures that we believe will address GAO's concerns.

SSA's field offices and SSA's regional disclosure coordinators already have authority to respond to a proper law enforcement request. Our field office employees use specific instructions in our POMS to respond quickly as requests come in. They may also consult with our regional disclosure coordinators located in each region, should additional questions arise. However, we have concerns about the recommendation to delegate "decision-making authority for law enforcement requests to specified locations such as the OIG...." As mentioned in the report, pursuant to the existing MOU between the Commissioner and the Inspector General (IG), the IG has administrative authority to make limited disclosures, which is different from decision-making authority. Under the Inspector General Act of 1978, agencies are expressly prohibited from transferring programmatic functions to Inspectors General. 5 U.S.C. app. 3 § 9(a)(2). In our view, delegation to the OIG of decision-making authority would not be permitted by the IG Act.

Recommendation 2

The Commissioner of SSA should provide law enforcement with information on SSA's disclosure policy and procedures.

Comment

We agree and we believe we have done so. As stated above, our POMS and privacy policies are available to the law enforcement community and the public. We note that the survey data indicates that most law enforcement entities are pleased by our service. However, we will review our Web site and other public informational materials to see if additional material or formatting changes would be helpful.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Shelia Drake (202) 512-7172 (drakes@gao.gov)
Jacqueline Harpp (202) 512-8380 (harppj@gao.gov)

Staff Acknowledgments

In addition to those named above, Margaret Armen, Richard Burkard, Malcolm Drewery, Kevin Jackson, Corinna Nicolaou, and David Plocher made key contributions to this report. Barbara Hills, Theresa Mechem, and Mimi Nguyen provided assistance with graphics.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER