United States General Accounting Office

GAO

Report to Congressional Requesters

May 2002

SOCIAL SECURITY NUMBERS

Government Benefits from SSN Use but Could Provide Better Safeguards

GAO-02-352

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
00MAY2002	N/A	-

Title and Subtitle SOCIAL SECURITY NUMBERS: Government Benefits from SSN Use but Could Provide Better Safeguards	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) U.S. General Accounting Office 441 G Street NW, Room LM Washington, D.C. 20548	**Performing Organization Report Number** GAO-02-352
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
The Social Security number (SSN) was created in 1936 as a means to track workers earnings and eligibility for Social Security benefits. Since that time, the number has been used for myriad non-Social Security purposes. Private sector use of the SSN has grown exponentially. For example, businesses may ask individuals to provide their SSNs when they apply for credit, seek medical or other insurance coverage, rent an apartment, or place an order for merchandise. In addition, many federal, state, and local government agencies also use the SSN. In some cases, these government agencies use SSNs as they administer their programs to deliver services or benefits to the public. Individuals who provide SSNs to receive these services and benefits may expect the SSNs to be considered confidential and thus protected from public disclosure. In other cases, government agencies serve as the repository for records or documents that are routinely made available to the public for inspection. These public records may contain SSNs.1

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR

Number of Pages
67

Contents

Figures

Abbreviations

DOD	Department of Defense
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
IRS	Internal Revenue Service
OMB	Office of Management and Budget
SSA	Social Security Administration
SSI	Supplemental Security Insurance
SSN	social security number
TANF	Temporary Assistance for Needy Families

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 31, 2002

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

The Honorable Dianne Feinstein, Chair
The Honorable Jon Kyl, Ranking Member
Subcommittee on Technology, Terrorism,
and Government Information,
Committee on the Judiciary
United States Senate

The Honorable Charles Grassley, Ranking Member
Subcommittee on Crime and Drugs,
Committee on the Judiciary
United States Senate

The Social Security number (SSN) was created in 1936 as a means to track workers' earnings and eligibility for Social Security benefits. Since that time, the number has been used for myriad non-Social Security purposes. Private sector use of the SSN has grown exponentially. For example, businesses may ask individuals to provide their SSNs when they apply for credit, seek medical or other insurance coverage, rent an apartment, or place an order for merchandise. In addition, many federal, state, and local government agencies also use the SSN. In some cases, these government agencies use SSNs as they administer their programs to deliver services or benefits to the public. Individuals who provide SSNs to receive these services and benefits may expect the SSNs to be considered confidential and thus protected from public disclosure. In other cases, government agencies serve as the repository for records or documents that are routinely made available to the public for inspection. These public records may contain SSNs.[1] This use of SSNs by the private sector and government agencies has raised public concern over how this personal information is

[1]We found no commonly accepted definition of public records. For the purposes of this report, when we use the term public record, we are referring to a record or document that is routinely made available to the public for inspection either by a federal, state, or local government agency or a court, such as those readily available at a public reading room, clerk's office, or on the Internet.

being used and protected. Further, the growth in electronic record keeping and the explosion of the availability of information over the Internet, combined with an apparent rise in identity theft, have heightened this concern.

We have previously reported that certain public and private sector officials told us that SSNs play an important role in their ability to deliver services or conduct business.[2] In this report, you asked us to delve deeper into the government uses of SSNs. Specifically, we studied (1) the extent and nature of federal, state, and county government agencies' use of SSNs as they administer programs to provide benefits and services; (2) the actions government agencies take to safeguard these SSNs from improper disclosure and use when they are used to administer programs; (3) the extent and nature of federal, state, and county governments' use of SSNs when they are contained in public records; and (4) the options available to better safeguard SSNs that are found in these public records.

To address these issues we interviewed knowledgeable federal, state, and county officials to identify government programs or activities that frequently use SSNs. To develop information on the nature and extent of governments' use of SSNs and their actions to protect individuals' privacy when using SSNs, we mailed surveys to 18 federal agencies and those departments that typically use SSNs in all 50 states, the District of Columbia, and the 90 most populous counties.[3] We also conducted site visits and in-depth interviews at six selected federal programs, three states, and three counties. We met with officials responsible for programs, agencies, or departments (hereinafter referred to generically as agencies) and courts that make frequent use of SSNs. We report on only those government entities that obtain, receive, or use SSNs. The information they provided was self-reported, and we did not verify it. We conducted our work between February 2001 and March 2002 in accordance with

[2] U.S. General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28 (Washington, D.C.: Feb. 16, 1999).

[3] We did not survey state Departments of Motor Vehicles or state agencies that administer state tax programs because we have reported on these activities separately. Nor did we focus on the requirements for the use and dissemination of taxpayer information because they are distinct from many of the requirements covered in this report. See U.S. General Accounting Office, *Child Support Enforcement: Most States Collect Drivers' SSNs and Use Them to Enforce Child Support*, GAO-02-239 (Washington, D.C.: Feb. 15, 2002) and *Taxpayer Confidentiality: Federal, State, and Local Agencies Receiving Taxpayer Information*, GAO-GGD-99-164 (Washington, D.C.: Aug. 30, 1999).

generally accepted government auditing standards. For additional information on our approach, please see appendix 1.

Results in Brief

When federal, state, and county government agencies administer programs that deliver services and benefits to the public, they rely extensively on the SSNs of those receiving the benefits and services. Because SSNs are unique identifiers and do not change, the numbers provide a convenient and efficient means of managing records. They are also particularly useful for data sharing and data matching because agencies can use them to check or compare their information quickly and accurately with that from other agencies. In so doing, these agencies can better ensure that they pay benefits or provide services only to eligible individuals and can more readily recover delinquent debts individuals may owe. Using SSNs for these purposes can save the government and taxpayer hundreds of millions of dollars each year and help make sure programs are achieving their goals. In addition to using SSNs to deliver services or benefits, agencies also use or share SSNs to conduct statistical programs, research, and program evaluations. Moreover, all government departments or agencies use their employees' SSNs to varying extents to perform some of their responsibilities as employers, such as paying their employees and providing health and other insurance benefits. In the course of using SSNs to administer their programs and as employers, agencies sometimes display these SSNs on documents, such as program eligibility cards or employee badges, that can be seen by others who may have no need for the SSN.

While government agencies are making wide use of SSNs, they are also taking some steps to safeguard the numbers; however, certain measures that could help protect SSNs are not uniformly in place at any level of government. First, when requesting SSNs, government agencies are not consistently providing individuals with information required by federal law. This information, such as how the SSNs will be used and whether individuals are required to provide their SSNs, is the first line of defense against improper disclosure because it allows SSN holders to make informed decisions about whether to provide their SSN to obtain the services in question. Second, although agencies that use SSNs to provide benefits and services are taking steps to safeguard the numbers from improper disclosure, our survey identified potential weaknesses in the security of information systems at all levels of government. Similarly, regarding the display of SSNs by these agencies, we found numerous examples of actions taken to limit the presence of SSNs on documents that are not intended to be public but are nonetheless seen by others; however,

these changes are not systematic and many government agencies continue to display SSNs on a variety of documents.

Regarding public records, many of the state and county agencies responding to our survey reported maintaining records that contain SSNs; however, federal program agencies maintain public records less frequently. At the state and county levels, certain offices, such as state professional licensing agencies and county recorders' offices, have traditionally been repositories for public records that may contain SSNs. These records chronicle the various life events and other activities of individuals as they interact with the government, such as birth certificates, professional licenses, and property title transfers. Officials who maintain these records told us their primary responsibility is to preserve the integrity of the record rather than protect the privacy of the individual SSN holder. In addition, courts at all three levels of government maintain public records that may contain SSNs, such as divorce decrees and child support orders. In some cases, government agencies and the courts create these documents containing SSNs themselves. In other cases, the documents are submitted by others, such as when title companies submit documents to support property title transfers and when attorneys submit evidence for the record. Traditionally, the general public has gained access to public records by visiting the office that maintains the records, which offers at least some practical limitations on the volume of SSNs any one person can collect. However, the growth of electronic record keeping has made it easier for a few agencies to provide or even sell their data in bulk. Moreover, although few entities report making SSNs available on the Internet, several officials told us they are considering expanding the volume and type of public records available on their Web site.

When SSNs have been found in public records, some government agencies are trying to better safeguard the SSN by trying innovative approaches to protect the SSNs from public display. For example, some agencies and courts are modifying their processes or their forms so that they can collect SSNs but prevent the number from becoming part of the publicly available record. This is most effective when the agency or court prepares the document. When others submit the document to become part of the public record, it is more difficult to limit the appearance of the SSN unless the individual or business submitting the document takes the initiative to omit the SSN or include it only when absolutely necessary. Regarding placing public records containing SSNs on Web sites, some agencies and courts have decided to limit this practice as well; however, some have not. Overall, the most far-reaching efforts we identified took place in states where there was a statewide initiative that established a policy and

procedures designed to protect individuals' personal information, including SSNs, in all of the different circumstances that governments collect, store, and use it.

We are making recommendations in this report that the Office of Management and Budget (OMB) direct federal agencies to review their practices for securing SSNs and providing SSN holders with information required by federal law and that OMB take steps to better inform state and local government agencies that they are required to provide this information when they request an individual's SSN. We are also presenting a matter for congressional consideration, suggesting that the Congress, in consultation with the president, convene a representative group of federal, state, and local officials to develop a unified approach to safeguarding SSNs used in government and particularly those displayed in public records. The Social Security Administration (SSA) and OMB generally agreed with our recommendations.

Background

Since the creation of the SSN, the number of federal agencies and others that rely on it has grown beyond the original intended purpose, in part because a number of federal laws authorize or require SSN use. Additionally, the advent of computerized records further increased reliance on SSNs. This growth in use and availability of SSNs is important because SSNs are often the "identifier" of choice among thieves who steal another individual's identity. Although no single federal law regulates overall use and disclosure of SSNs by governments, when federal government agencies use SSNs, several federal laws limit the use and disclosure of the number in certain circumstances.[4] Also, state laws may vary in terms of the restrictions imposed on SSN use and disclosure. Moreover, some records that contain SSNs are considered part of the public record and, as such, are routinely made available to the public for review.

Use of SSN Has Grown, in Part, Because of Federal Requirements

SSA is the federal agency responsible for issuing SSNs, which are used to track workers' earnings and eligibility for Social Security benefits. Legislation enacted in 1935 created the SSA and made the agency responsible for implementing a social insurance program designed to pay

[4] In this review, we do not include criminal provisions that might apply to the improper use of SSNs.

benefits to retired workers to ensure a continuing portion of income after retirement.[5] The amount of these benefits was based, in part, on the amount of the workers' earnings. As a result, SSA needed a system to keep track of earnings by individual worker and for employers to report these earnings. In 1936, SSA created a numbering system designed to provide a unique identifier, the SSN, to each individual. Workers are now required by law to provide SSA their number when they apply for benefits from SSA. As of December 1998, SSA had issued 391 million SSNs.

Since the creation of the SSN, other entities in both the private and public sectors have begun using SSNs, in part because of federal requirements. Widespread SSN use in government began with a 1943 Executive Order issued by President Franklin D. Roosevelt requiring that all federal agencies use the SSN exclusively when agencies need to use identification systems for individuals, rather than set up a new identification system. In later years, the number of federal agencies and others relying on the SSN as a primary identifier escalated dramatically, in part, because a number of federal laws were passed that authorized or required its use for specific activities as shown in table 1. In many instances, the laws required that SSNs be used to determine individuals' eligibility for certain federally funded program services or benefits, or they served as a unique identifier for such government-related activities as paying taxes or reporting wages earned. In some cases these statutes require that state and local governmental entities collect SSNs.

[5] The Social Security Act of 1935 created the Social Security Board, which was renamed the Social Security Administration in 1946.

Table 1: Examples of Federal Statutes That Authorize or Mandate the Collection and Use of Social Security Numbers

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Tax Reform Act of 1976 42 U.S.C. 405(c)(2)(c)(i)	General public assistance programs, tax administration, driver's license, motor vehicle registration	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver's license, or motor vehicle registration law
Food Stamp Act of 1977 7 U.S.C. 2025(e)(1)	Food Stamp Program	Mandates the secretary of agriculture and state agencies to require SSNs for program participation
Deficit Reduction Act of 1984 42 U.S.C. 1320b-7(1)	Eligibility benefits under the Medicaid program	Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program
Housing and Community Development Act of 1987 42 U.S.C. 3543(a)	Eligibility for the Department of Housing and Urban Development programs	Authorizes the secretary of the Department of Housing and Urban Development to require program applicants and participants to submit their SSNs as a condition of eligibility
Family Support Act of 1988 42 U.S.C. 405(c)(2)(C)(ii)	Issuance of birth certificates	Requires states to obtain parents' SSNs before issuing a birth certificate unless there is good cause for not requiring the number
Technical and Miscellaneous Revenue Act of 1988 42 U.S.C. 405(c)(2)(D)(i)	Blood donation	Authorizes states and political subdivisions to require that blood donors provide their SSNs
Food, Agriculture, Conservation, and Trade Act of 1990 42 U.S.C. 405(c)(2)(C)	Retail and wholesale businesses participation in food stamp program	Authorizes the secretary of agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps
Omnibus Budget Reconciliation Act of 1990 38 U.S.C. 510(c)	Eligibility for Veterans Affairs compensation or pension benefits programs	Requires individuals to provide their SSNs to be eligible for Department of Veterans Affairs' compensation or pension benefits programs
Social Security Independence and Program Improvements Act of 1994 42 U.S.C. 405(c)(2)(E)	Eligibility of potential jurors	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors
Personal Responsibility and Work Opportunity Reconciliation Act of 1996 42 U.S.C. 666(a)(13)	Various license applications, divorce and child support documents, death certificates	Mandates that states have laws in effect that require collection of SSNs on applications for driver's licenses and other licenses; requires placement in the pertinent records of the SSN of the person subject to a divorce decree, child support order, paternity determination; requires SSNs on death certificates; creates national database for child support enforcement purposes
Debt Collection Improvement Act of 1996 31 U.S.C. 7701(c)	Persons doing business with a federal agency	Requires those doing business with a federal agency (i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, right-of-ways, grants, or benefit payments; contractors of an agency and others) to furnish SSNs to the agency
Higher Education Act Amendments of 1998 20 U.S.C. 1090(a)(7)	Financial assistance	Authorizes the secretary of education to include the SSNs of parents of dependent students on certain financial assistance forms
Internal Revenue Code (various amendments) 26 U.S.C. 6109	Tax returns	Authorizes the commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns

Source: GAO review of applicable federal laws

Private businesses, such as financial institutions and health care service providers, also frequently ask individuals for their SSNs. In some cases, they require the SSN to comply with federal laws but at other times, these businesses routinely choose to use the SSNs to conduct business. SSNs are a key piece of identification in building credit bureau databases, extracting or retrieving data from consumers' credit histories, and preventing fraud. Businesses routinely report consumers' financial transactions, such as charges, loans, and credit repayments to credit bureaus. A representative for the credit bureaus estimated that 80 percent of these transactions include SSNs. Although the representative reported that credit bureaus use other identifiers, such as names and addresses, to build and maintain individuals' credit histories, credit bureaus view the SSN as one of the most important identifiers for ensuring that correct information is associated with the right individual because the SSN does not change as would a name or address. The credit bureaus' representative told us that without the SSN, or a similar stable identifier, such as a biometric identifier, [6] credit bureaus could still conduct business but the level of accuracy of individuals' credit records would be greatly reduced. The fundamental goal of credit bureaus is ensuring that the credit information provided to those who grant consumers credit is accurate. The less accurate the information, the less value that information is to those who grant credit. The credit bureaus' representative told us that until other stable identifiers like biometrics gain widespread use, credit bureaus view the SSN as the key tool for ensuring the accuracy of consumer credit histories.

The advent of computerized record keeping has implications for the availability of SSNs and other sensitive data. Government entities are beginning to make their records electronically available over the Internet. Moreover, the Government Paperwork Elimination Act of 1998 requires that, where practicable, federal agencies provide by 2003 for the option of the electronic maintenance, submission, or disclosure of information. State government agencies have also initiated Web sites to address electronic government initiatives. Moreover, continuing advances in computer technology and the ready availability of computerized data have spurred the growth of new business activities that involve the compilation

[6] Biometric identification uses automated methods of recognizing a person based on a physiological or behavioral characteristic including fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins.

of vast amounts of personal information about members of the public, including SSNs, that businesses sell.

Identity Thieves Often Use Others' SSNs

This growth in the use of SSNs is important to individual SSN holders because these numbers, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves.[7] Identity theft is a crime that can affect all Americans. It occurs when an individual steals another individual's personal identifying information and uses it fraudulently. For example, SSNs and other personal information are used to fraudulently obtain credit cards, open utility accounts, access existing financial accounts, commit bank fraud, file false tax returns, and falsely obtain employment and government benefits. SSNs play an important role in identity theft because they are used as breeder information to create additional false identification documents, such as drivers' licenses.

Most often, identity thieves use SSNs belonging to real people rather than making one up; however, on the basis of a review of identity theft reports, victims usually (75 percent of the time) did not know where or how the thieves got their personal information.[8] In the 25 percent of the time when the source was known, the personal information, including SSNs, usually was obtained illegally. In these cases, identity thieves most often gained access to this personal information by taking advantage of an existing relationship with the victim. The next most common means of gaining access were by stealing information from purses, wallets, or the mail. In addition, individuals can also obtain SSNs from their workplace and use them or sell them to others. Finally, SSNs and other identifying information can be obtained legally through Internet sites maintained by both the public and private sectors and from records routinely made available to the public by government entities and courts. Because the sources of identity theft cannot be more accurately pinpointed, it is not possible at this time to determine whether SSNs that are used improperly are obtained most frequently from the private sector or the government.

[7] United States Sentencing Commission, *Identity Theft Final Alert* (Washington, D.C.: Dec. 15, 1999).

[8] This information is based on a review of 39 cases involving SSN theft drawn from the Federal Trade Commission's fiscal year 1998 data files.

Recent statistics collected by federal and consumer reporting agencies indicate that the incidence of identity theft appears to be growing.[9] The Federal Trade Commission (FTC), the agency responsible for tracking identity theft, reports that complaint calls from possible victims of identity theft grew from about 445 calls per week in November 1999, when it began collecting this information, to about 3,000 calls per week by December 2001. However, FTC noted that this increase in calls might also, in part, reflect enhanced consumer awareness. In addition, SSA's Office of the Inspector General, which operates a fraud hotline, reports that allegations of SSN misuse increased from about 11,000 in fiscal year 1998 to more than 65,200 in fiscal year 2001. Additionally, SSA reported that almost 39,000 other allegations of program fraud also include an element of SSN misuse during fiscal year 2001. Most of these allegations relate to identity theft. However, some of the reported increase may be a result of a growth in the number of staff SSA assigned to field calls to the Fraud Hotline during this period. SSA staff increased from 11 to over 50 during this period, which allowed personnel to answer more calls. Also, officials from two of the three national consumer reporting agencies report an increase in the number of 7 year fraud alerts placed on consumer credit files, which they consider to be reliable indicators of the incidence of identity theft.[10] Finally, it is difficult to determine how many individuals are prosecuted for identity theft because law enforcement entities report that identity theft is almost always a component of other crimes, such as bank fraud or credit card fraud, and may be prosecuted under the statutes covering those crimes.

In Some Instances SSNs are to Be Protected from Public Disclosure

No single federal law regulates the overall use or restricts the disclosure of SSNs by governments; however, a number of laws limit SSN use in specific circumstances. Generally, the federal government's overall use and disclosure of SSNs are restricted under the Freedom of Information Act (FOIA) and the Privacy Act. Broadly speaking, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against

[9] U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

[10] A fraud alert is a warning that someone may be using the consumer's personal information to fraudulently obtain credit. When a fraud alert is placed on a consumer's credit card file, it advises credit grantors to conduct additional identity verification before granting credit. The third consumer reporting agency offers fraud alerts that can vary from 2 to 7 years at the discretion of the individual.

unwarranted invasions of their privacy by federal agencies. Also, the Social Security Act Amendments of 1990 also provide some limits on disclosure, and these limits apply to state and local governments as well. In addition, a number of federal statutes impose certain restrictions on SSN use and disclosure for specific programs or activities.[11] At the state and county level, each state may have its own statutes addressing the public's access to government records and privacy matters; therefore, states may vary in terms of the restrictions they impose on SSN use and disclosure. Table 2 shows key laws that may affect SSN disclosure at the federal, state, and county level. For more information on the specific provisions in the federal laws, including a summary of the privacy principles that underlie the Privacy Act, see appendix II.

Table 2: Comparison of Key Provisions Concerning Disclosure of SSNs

Federal	State	County
The Freedom of Information Act of 1966– presumes government records are available upon formal request, but exempts certain personal information, such as SSNs	Open records laws or "sunshine" laws—vary by state but all 50 states and the District of Columbia have such statutes	Governed by state and/or local laws
The Privacy Act of 1974– regulates certain types of federal recordkeeping; generally prohibits disclosure of personal information, such as SSNs, with exceptions	A number of states have enacted their own privacy laws or they rely on other guidance; at least 17 states have statutes that specifically address SSN use or disclosure	Governed by state and/or local laws
The Social Security Act Amendments of 1990 –bars disclosure of SSNs collected because of laws enacted on or after October 1, 1990	The Social Security Act Amendments of 1990	The Social Security Act Amendments of 1990

Source: GAO review of federal laws, and The Privacy Journal, Compilation of State and Federal Laws, 1997 edition with updates in a1999 Supplement and a 2000 Supplement.

In addition, a number of laws provide protection for sensitive information, such as SSNs, when maintained in computer systems and other government records. Most recently, the Government Information Security Reform provisions of the Fiscal Year 2001 Defense Authorization Act require that federal agencies take specific measures to safeguard

[11] For example, the Internal Revenue Code, which requires the use of SSNs for certain purposes, declares tax return information, including SSNs, to be confidential, limits access to specific organizations, and prescribes both civil and criminal penalties for unauthorized disclosure. For more information, see GAO-GGD-99-164. Also, the Personal Responsibility and Work Opportunity Act of 1996 explicitly restricts the use of SSNs to purposes set out in the Act, such as locating absentee parents to collect child support payments.

computer systems that may contain SSNs. [12] For example, federal agencies must develop agency-wide information security management programs, establish security plans for computer systems, and conduct information security awareness training for employees. These laws do not apply to state and local governments; however, in some cases state and local governments have developed their own statutes or put requirements in place to similarly safeguard sensitive information, including SSNs, kept in their computer systems.

SSNs Are Found in Some Public Records

In some cases, government entities, particularly at the state and county levels, maintain public records that are routinely made available to the public for inspection. For state and county executive branch agencies, state law generally governs whether and under what circumstances these records are made available to the public, and they vary from state-to-state. Records may be made available for a number of reasons. These include the presumption that citizens need government information to assist in oversight and ensure that government is accountable to the people. In addition, some government agencies, such as county clerks or recorders, exist primarily to create or maintain records to assist the public and private sector in the conduct of business, legal, or personal affairs. These records may contain SSNs.

Certain records maintained by the federal, state, and county courts are also made available to the public. In principle, these records are open to aid in preserving the integrity of the judicial process and to enhance the public trust and confidence in the judicial process. Courts are generally not subject to FOIA or other open record laws. At the federal level, access to court documents generally has its grounding in common law and constitutional principles. In some cases, public access is also required by statute, as is the case for papers filed in a bankruptcy proceeding. As with federal courts, requirements regarding access to state and local court records may have a state common law or constitutional basis or may be based on state laws. Although states' laws may vary, generally, custodians of court records must identify a statute, court rule, or a case law or common law basis to preclude public access to a particular record;

[12] These provisions supplement information security requirements established in the federal Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and Office of Management and Budget guidance.

otherwise the record is presumed to be accessible to the public and must be disclosed to the public upon request.

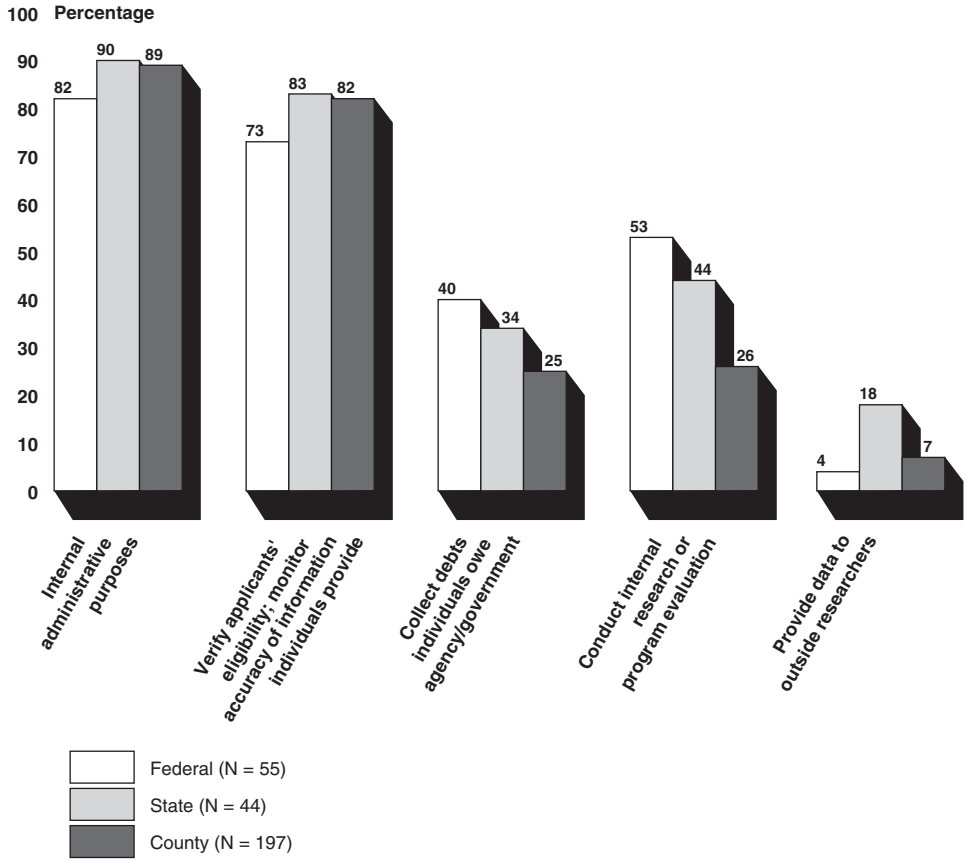
All Levels of Governments Use SSNs Extensively for a Wide Range of Purposes

SSNs are widely used by federal, state, and county government agencies when they provide services and benefits to the public. These agencies use SSNs both to manage their records and to facilitate data sharing with others. They share SSNs and other personal information to verify eligibility for benefits, collect debts owed the government, and conduct or support research and evaluation. In addition to using SSNs for program purposes, many of these agencies also reported using their employees' SSNs for activities such as payroll, wage reporting, and providing employee benefits. As a result of this widespread SSN usage, these agencies occasionally display SSNs on documents that may be viewed by others who do not have a need for this personal information.

Agencies Use SSNs to Administer Programs That Provide Benefits or Services to Individuals

Most of the agencies we surveyed at all levels of government reported using SSNs extensively to administer their programs. As shown in figure 1, more agencies reported using SSNs for internal administrative purposes, that is, they use them to identify, retrieve, and update their records, than for any other purpose. SSNs are so widely used for this purpose, in part, because each number is unique to an individual and does not change, unlike some other personal identifying information, such as names and addresses. For this reason, SSNs can provide a convenient and efficient means to manage records, particularly electronic records, that catalog services or benefits government agencies provide individuals or families.

Figure 1: Percentage of Program Agencies Using SSNs for Each Reason Listed



Legend: N is the number of respondents upon which the percentage is based.

Source: GAO surveys of federal, state, and county departments and agencies. Figure includes departments and agencies that administer programs and excludes courts, county clerks and recorders, and state licensing agencies.

Many agencies also use SSNs to share information with other entities to bolster the integrity of the programs they administer. For example, individuals are often asked to report their income, citizenship status, and household composition to determine their eligibility for government benefits or services. To avoid paying benefits or providing services or loans to individuals who are not really eligible for them, agencies use applicants' SSNs to match the information they provide with information in other data bases, such as other federal benefit paying agencies, state unemployment agencies, the Internal Revenue Service (IRS), or employers. As unique identifiers, SSNs help ensure that the agency is obtaining or matching information on the correct person.

SSNs Are Used to Verify Eligibility

As shown in figure 1, the majority of agencies at all three levels of government reported sharing information containing SSNs for the purpose of verifying an applicant's eligibility for services or benefits. These data-sharing activities can help save the government and taxpayers hundreds of millions of dollars. In some cases, the Congress has recognized the benefits of this data sharing for federally funded programs and has either explicitly permitted or required agencies to share data for these purposes. Examples of SSN use for verifying and monitoring eligibility include the following:

- Individuals confined to a correctional facility for at least 1 full month are ineligible to continue receiving federal Supplemental Security Income (SSI) program benefits.[13] SSA, the federal agency that administers this program, uses SSNs to match records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments. We reported that between January and August 1996, the sharing of prisoner data between SSA and state and local correctional facilities helped SSA identify about $151 million overpayments already made and prevented about $173 million in additional overpayments to ineligible prisoners.[14]

- When individuals apply for Temporary Assistance for Needy Families (TANF), a program designed to help low-income families, the law requires them to provide program administrators their SSNs and information about their income and resources.[15] Some agencies that administer this program use SSNs to share data to determine the applicants' and current recipients' eligibility and to verify self-reported information. The state of New York alone estimated that by checking state wage data records, it saved about $72 million in unpaid benefits between January and September 1999.[16]

[13] SSI provides cash assistance to needy individuals who are aged, blind, or disabled.

[14] U.S. General Accounting Office, *Supplemental Security Income: Incentive Payments Have Reduced Benefit Overpayments to Prisoners*, GAO/HEHS-00-2 (Washington, D.C.: Nov. 22, 1999).

[15] TANF was created by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996. The program has been implemented in the form of block grants to states and is designed to help low-income families with children reduce their reliance on welfare and move toward economic independence.

[16] U.S. General Accounting Office, *Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity*, GAO/HEHS-00-119 (Washington, D.C.: Sept. 13, 2000).

SSNs Are Used to Collect Debt

SSNs can also help ensure program integrity when they are used to collect delinquent debts, and some agencies at each level of government reported sharing data containing SSNs for this purpose. Individuals may owe such debts to government agencies when they fall behind in loan repayments, have underpaid taxes, or are found to have fraudulently received benefits. For example:

- The Department of Education uses SSNs to match data on defaulted education loans with the National Directory of New Hires. This database, which was implemented in October 1997, contains the names and SSNs, among other information, of individuals that employers reported hiring after implementation.[17] As a result of this matching, which was implemented in fiscal year 2001, the department reported collecting $130 million from defaulted student loans borrowers in 2001.

- The Department of the Treasury, as the federal government's lead agency for debt collection, also uses the SSN. For example, when an individual falls behind in payments owed the federal government, the agency owed the debt provides Treasury with the debtors' SSN and debt information. Treasury then uses the SSN to determine whether individuals owe the federal government money before making certain payments, such as tax refunds. If Treasury finds the individual is delinquent in paying a debt to the government, the agency will offset certain payments due the individual to satisfy the debt. Using this approach, Treasury used tax refund offsets to collect over $1 billion in federal nontax debt in 2001.

SSNs Are Used for Statistics, Research, and Evaluation

Certain statistical agencies, which are responsible for collecting and maintaining data for statistical programs that are required by statute, make use of SSNs. In some cases, these data are compiled using information provided for another purpose. For example, the Bureau of the Census prepares annual population estimates for states and counties using individual income tax return data linked over time by SSN to determine

[17] The Department of Health and Human Services' National Directory of New Hires is a national database containing new hire and wage data from every state and federal agency and unemployment insurance data from state unemployment security agencies. This directory was mandated by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 to help enforce child support obligations. At a minimum, the database includes the individual's name, address, and SSN, as well as the employer's name, address, and identification number. This data is also used for various program enforcement purposes by a limited number of state and federal agencies.

migration rates between localities.[18] For its Survey of Income and Population Participation, the bureau asks survey participants for various demographic characteristics and types of incomes received. The bureau also asks participants to provide their SSNs, informing them that the SSNs will be used to obtain information from other government agencies to avoid asking for information already reported to the government. As is the case for all government information collections, OMB must approve the collection of data for such statistical and research purposes.

In addition, SSNs along with other program data, are sometimes used for research and evaluation. SSNs provide government agencies and others with an effective mechanism for linking data on program participation with data from other sources to help evaluate the outcomes or effectiveness of government programs.[19] This information can prove invaluable to program administrators as well as policymakers. As shown in table 3, more than one-third of federal, state, and county agencies combined reported using SSNs to conduct internal research or program evaluation, and almost one-fifth of state agencies provide data containing SSNs to outside researchers. Examples of SSN use for evaluation and research include the following:

- As one of its many uses, Census may match the Survey of Income and Population Participation responses with data contained in records for programs such as TANF, Supplemental Security Income, and food stamp programs. Linking various data by SSN helps policymakers assess the extent to which these federal programs together assist low-income individuals.

- Health departments may provide SSN information to outside researchers, including universities or foundations, or provide SSN information to other organizations such as the National Center for Health Statistics, which compile national data on subjects such as infant birth and mortality data.

[18] Census is authorized by statute to collect a variety of information, and the Bureau is also prohibited from making it available, except in certain circumstances.

[19] In some cases, records containing SSNs are sometimes matched across multiple agency or program databases. The statistical and research communities refer to the process of matching records containing SSNs for statistical or research purposes as "record linkage." See U.S. General Accounting Office, *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information*, GAO-01-126SP (Washington, D.C.: Apr. 2001).

Other Program Uses

In addition to the above reasons for sharing data that focus primarily on program integrity and research, some agencies use SSNs as a means of sharing data to improve services. For example, in light of major changes to the nation's welfare program in 1996, welfare agencies are focusing on moving needy families toward economic independence and are drawing on numerous federal and state programs to provide a wide array of services, such as child care, food stamps, and employment and training. Sharing data can help them identify what services beneficiaries have received and what additional services are available or needed.

Agencies Are Most Likely to Share SSNs with Other Government Agencies and Contractors

All government agencies that administer programs and share records containing individuals' SSNs with other entities reported sharing SSNs with at least one other government agency.[20] Aside from sharing with other government agencies, the largest percentage of federal and state program agencies report sharing SSNs with contractors, and a relatively large percentage of county program agencies report sharing with contractors as well, as shown in table 3. Agencies across all levels of government use contractors to help them fulfill their program responsibilities. Contractors most frequently determine eligibility for services, provide services, conduct data processing activities, and perform research and evaluation. In addition to sharing SSNs with contractors, government agencies also share SSNs with private businesses, such as credit bureaus and insurance companies, as well as debt collection agencies, researchers, and, to a lesser extent, with private investigators.

[20] On the federal level, data sharing often involves computerized record matching. The Computer Matching and Privacy Protection Act of 1988, which amended the Privacy Act, specifies procedural safeguards affecting agencies' use of Privacy Act records in performing certain types of computerized matching program, including due process rights for individuals whose records are being matched. These due process rights were further clarified in the Computer Matching and Privacy Protection Amendments of 1990.

Table 3: Of Program Agencies That Share SSNs, Percentage That Share Them with Specific NonGovernment Entities

Entities That Receive SSNs from Government agencies	Government Agencies Reporting Sharing SSNs		
	Federal	State	County
Contractors	**54%**	**39%**	**28%**
	(39)	(149)	(138)
Credit bureaus	**31%**	**17%**	**10%**
	(32)	(145)	(138)
Insurance companies	**24%**	**28%**	**31%**
	(33)	(147)	(139)
Debt collection agencies	**29%**	**16%**	**10%**
	(31)	(140)	(136)
Researchers	**12%**	**33%**	**14%**
	(34)	(147)	(135)
Private investigators	**0%**	**7%**	**7%**
	(0)	(141)	(138)
Marketing companies	**0%**	**2%**	**1%**
	(0)	(139)	(137)

Legend: The number in parentheses is the number of respondents upon which the percentage is based.

Source: GAO survey of federal, state, and county agencies, using responses from those that reported sharing SSNs. Table includes departments and agencies that administer programs for the public and excludes courts, county clerks and recorders, and state licensing agencies.

Governments Use Employees' SSNs for Employer-Related Activities

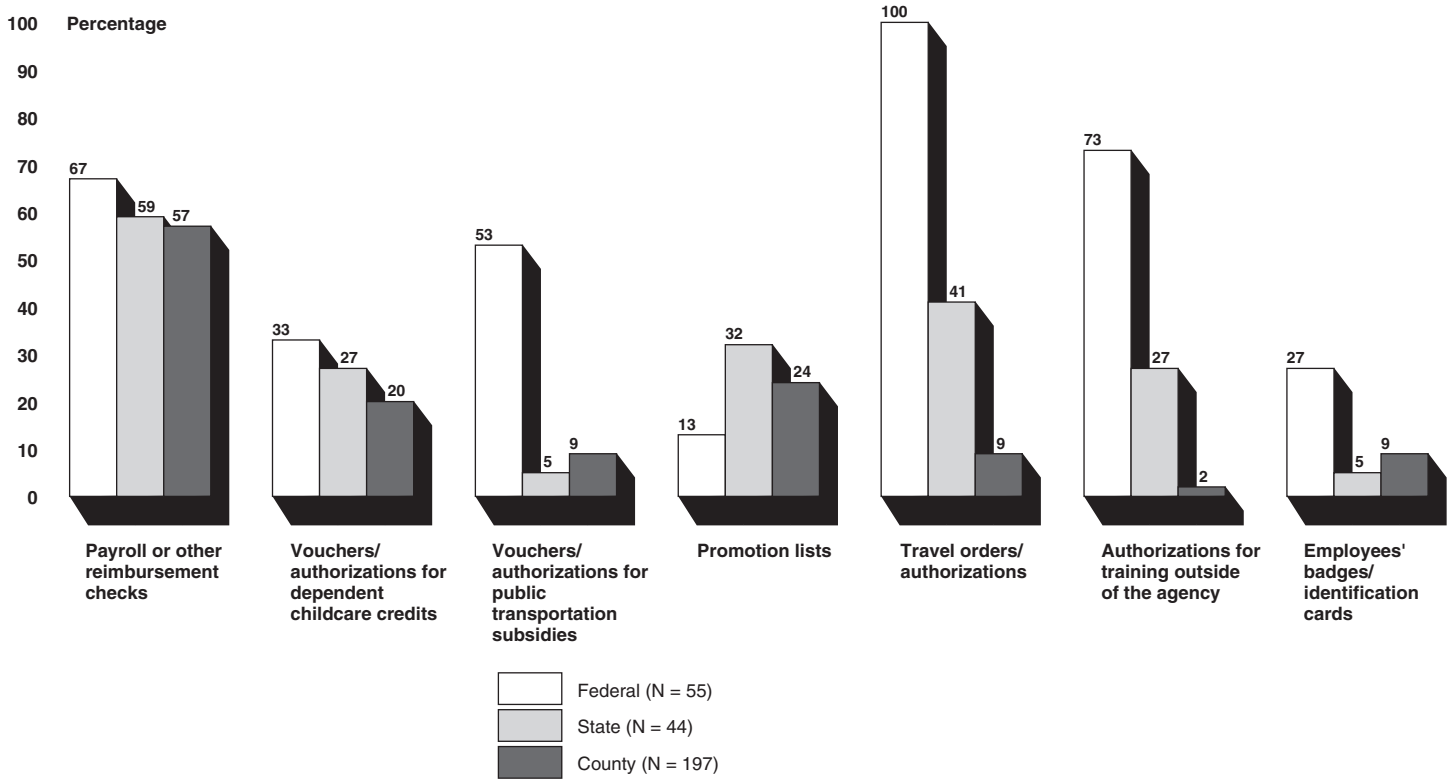
All government personnel departments we surveyed reported using their employees' SSNs to fulfill at least some of their responsibilities as employers. As with many of the program-related SSN uses described earlier, these employer uses involve data sharing among governments and other agencies. Personnel departments responding to our questionnaire said they use SSNs to help them maintain internal records and provide employee benefits. To provide these benefits, employers often share data on employees with other entities, such as health care providers or pension plan administrators. As an example, employers submit employees' SSNs along with certain information about employees to health insurers and retirement plan administrators. Health insurers may use the SSNs to identify enrollment in health plans and verify eligibility for payments for health services. Retirement plan administrators use the SSN to record the contribution in the correct employee account, and when they make payments to individuals, they are required to report the payments using the individuals' SSNs to the IRS.

In addition, employers are required by law to use employees' SSNs when reporting wages. Wages are reported to SSA, and the agency uses this information to update earnings records it maintains for each individual. These earnings ultimately determine eligibility for and the amount of Social Security benefits. After processing these reported wages, SSA provides the information to the IRS, which uses it to monitor individuals' compliance with the federal personal income tax rules. The IRS uses SSNs to match these employer wage reports with amounts individuals report on personal income tax returns. Finally, federal law requires that states maintain employers' reports of newly hired employees, identified by SSNs. States must forward this information to a national database that is used by state child support agencies to locate parents who are delinquent in child support payments.

Government Agencies Occasionally Display SSNs on Documents That May Be Viewed by Others

In the course of delivering their services or benefits, many government agencies occasionally display SSNs on documents that may be viewed by others, some of whom may not have a need for this personal information. Figure 2 shows a variety of ways SSNs are displayed, as reported in our survey by federal, state, and county personnel departments. When SSNs appear on payroll checks, rather than on the more easily safeguarded pay stub, any number of individuals can view the employee's SSN depending on where the check is cashed. To receive services at government rates, government employees may be required to provide hotel employees and others documents such as travel orders or tax exemption forms that display their SSNs.

Figure 2: Percentage of Government Personnel Departments That Display SSNs on Different Types of Documents



Legend: N is the number of respondents upon which the percentage is based.

Source: GAO surveys of federal, state, and county personnel administrators.

Some federal agencies and a few state and county personnel departments reported displaying employees' SSNs on their employee badges. Notably, the Department of Defense (DOD), which has over 2.7 million active and reserve military personnel, displays SSNs on its identification cards for these personnel. According to DOD officials, the Geneva Convention suggests that military personnel have an identification number displayed on their identification card, and DOD has chosen to use the SSN for this purpose. On the state level, the Department of Criminal Justice in one state, which has about 40,000 employees, displays SSNs on all employee identification cards. According to that state's Department of Criminal Justice officials, some of their employees have taken actions such as taping over their SSNs so that prison inmates and others cannot view this personal information.

SSNs are also displayed on documents that are not employee-related. For example, some benefit programs display the SSN on the benefit checks and eligibility cards, and over one-third of federal respondents reported including the SSN on official letters mailed to participants. Further, some state institutions of higher education display students' SSNs on identification cards. Finally, SSNs are sometimes displayed on business permits that must be posted in public view at an individual's place of business.

Governments Are Taking Some Steps to Safeguard SSNs but Important Measures Not Universally Employed

When agencies that deliver services and benefits use SSNs to administer programs, they are taking some steps to safeguard SSNs, but certain measures that could provide more assurances that these SSNs are secure are not universally in place at any level of government. First, when federal, state, and county agencies request SSNs, they are not consistently informing the SSN holders of whether they must provide the SSN to receive benefits or services and how the SSN will be used. In addition, although some agencies are using identifiers other than the SSNs in their records, most report it would be difficult to stop using SSNs. When agencies do use the SSN, we found weaknesses in their information systems security at all levels of government, which indicate SSNs may be at risk of improper disclosure. Finally, although some agencies are taking action to limit the display of SSNs on documents that are not intended to be public but may be viewed by others, these actions are sometimes taking place in a piecemeal manner rather than as a result of a systematic effort.

Many Government Entities Collect SSNs without Providing Required Information

When a government agency requests an individual's SSN, the individual needs certain information to make an informed decision about whether to provide their SSN to the government agency or not. Accordingly, section 7 of the Privacy Act requires that any federal, state, or local government agency, when requesting an SSN from an individual, provide that individual with three key pieces of information.[21] Government entities must

- tell individuals whether disclosing their SSNs is mandatory or voluntary,

[21] Section 7 of the Privacy Act is not codified with the rest of the act, but rather is found in the note section to 5 U.S.C. 552a.

- cite the statutory or other authority under which the request is being made, and

- state what uses government will make of the individual's SSN.

This information, which helps the individual make an informed decision, is the first line of defense against improper use.

Although nearly all government entities we surveyed collect and use SSNs for a variety of reasons, many of these entities reported they do not provide individuals the information required under section 7 of the Privacy Act when requesting their SSNs. As shown in table 4, federal agencies were more likely to report that they provided the required information to individuals when requesting their SSNs than were states or local government agencies. Even so, federal agencies did not consistently provide this required information; 32 percent reported that they did not inform individuals of the statutory authority for requesting the SSN and 21 percent of federal agencies reported that they did not inform individuals of how their SSNs would be used.

Table 4: Percentage of Government Entities That Provide Individuals with Required Information When Collecting SSNs

Informs Individuals	Federal	State	County
That providing SSN is voluntary	**90%**	**38%**	**42%**
	(10)	(78)	(74)
Of legal authority to request SSNs	**68%**	**51%**	**39%**
	(37)	(147)	(161)
How SSNs will be used	**79%**	**51%**	**36%**
	(57)	(270)	(294)

Legend: The number in parentheses is the number of respondents upon which the percentage is based.

Source: Data from GAO surveys of federal, state, and county departments, using responses from all government entities.

For federal agencies, OMB is responsible for assisting with and overseeing the implementation of the Privacy Act. Although OMB has issued guidance for federal agencies to follow in implementing the act overall, OMB's guidance does not address section 7.[22] However, there is another provision

[22] The Department of Justice has on its Web site an overview of the Privacy Act that references section 7. This information was prepared in coordination with OMB.

of the act that contains requirements similar to those of section 7, and OMB guidance does address this provision. [23] This provision requires agencies to inform individuals from whom they request information (1) the legal authority that authorizes the collection and whether disclosure is voluntary or mandatory, (2) the purposes for which the information is intended to be used, (3) the routine uses to be made of the information, and (4) the effects on the individual of not providing all or any part of the information. Agencies must provide this information on the forms they use to collect the information or on a separate form that can be retained by the individual. However, this provision differs from section 7 in important ways. It applies only to federal agencies that maintain a system of records, as defined under the act, whereas section 7 applies to all agencies at the federal, state, and local level and contains no provision limiting its coverage to agencies maintaining a system of records.[24]

Regarding how OMB oversees implementation of the Privacy Act, OMB officials told us that they review certain federal agency actions related to the Privacy Act, such as notices placed in the federal register to inform the public of changes to agency systems of records; however it is not their role to monitor day-to-day federal agency compliance with the many provisions of the act.[25] For this ongoing compliance monitoring, OMB officials said that they rely on agency privacy officers, general counsels, and inspector generals.[26] In addition, under the Act, individuals can bring a civil action against a federal agency requesting the SSN if they believe that the agency has not complied with the section 7 requirements and if this failure to comply results in an adverse effect on the individual.

At the state and county levels of government, it is not clear who has responsibility for overseeing the section 7 requirements placed on state

[23] 5 U.S.C. 552a(e)(3).

[24] Of the 58 federal programs that responded to our survey, 39 reported that some portion of their records were covered by the Privacy Act, 3 reported that no portion of their records were covered by the act, and the remaining 16 agencies did not know if their records were covered by the Privacy Act.

[25] Under the Paperwork Reduction Act, OMB is, however, responsible for reviewing and approving all collections of information including forms, surveys, telephonic requests, or various other formats used by federal agencies when requesting SSNs and other information from an SSN holder, state or local governments, and others. Thus the agency also has this opportunity to influence the collection of SSNs.

[26] According to OMB officials, all federal agencies have an officer responsible for implementing the Privacy Act.

and local governments. In fact, some state and local officials we spoke with were unaware of the requirements. Moreover, OMB officials told us that they have not issued any implementing regulations or guidance for section 7 for state and county government agencies, and no federal agency has assumed overall responsibility for monitoring these agencies and informing them of their obligations under section 7 of the Privacy Act.[27] According to OMB officials, their role with respect to state and local governments is limited to advising state and county officials who raise questions about the act. In addition, OMB officials also work with the National Association of State Chief Information Officers and other organizations to discuss and share ideas on information management issues.

Further, unlike the federal government, courts have disagreed on whether individuals have a right of civil action against state and county governments when these individuals believe state or county agencies are not complying with section 7 of the Privacy Act. For example, a Ninth Circuit Court of Appeals decision held that individuals do not have a right of action against state and local governments for violating the Privacy Act.[28] Conversely, other courts have recognized implied remedies against state governments for violations of the act. For example, in Louisiana, a district court ordered that the state stop asking for SSNs as a prerequisite to voter registration, based partially on the court's determination that the Louisiana commissioner of elections was violating section 7 of the act.[29] Similarly, a district court found that Virginia violated the act when collecting SSNs for voter registration because it did not provide required notice when requesting individuals' SSNs.[30]

[27] When federal agencies provide states with funding for specific programs, they could include requirements that the entities implementing the program comply with section 7 of the Privacy Act.

[28] *Dittman v. California*, 191 F.3d 1020 (9th Cir. 1999) (citing *Unt v. Aerospace Corp*, 765 F.2d 1440 (9th Cir. 1981)). The Ninth Circuit Court of Appeals covers California, Oregon, Washington, Arizona, Montana, Idaho, Nevada, Alaska, Hawaii, Guam, and the Northern Mariana Islands.

[29] *McKay v. Altobello*, No. 96-3458, 1997 WL 266717 (E.D. La. May 16, 1997).

[30] *Griedinger v. Davis*, 782 F. Supp. 1106 (E.D. Va. 1992), *reversed and remanded on other grounds*, 988 F.2d 1344 (4th Cir.1993).

More Can Be Done to Protect SSNs from Improper Public Disclosure

When government agencies collect SSNs that are not part of public records, they have a number of options available to them to limit the risk of improper disclosure. These agencies can

- use numbers other than SSNs for some program activities;
- implement a number of controls to ensure that when they use SSNs, they are properly safeguarded; and
- limit the use of SSNs on documents that may be viewed by others who do not have a need to access this personal information.

Some Agencies Use Alternate Numbers, but Most Report it Would Be Difficult to Stop Using SSNs

Despite the widespread use of SSNs at all levels of government, not all agencies use the SSN. Some respondents (19 from state departments and 33 from county departments) reported that they do not obtain, receive, or use the SSNs of program participants, service recipients, or individual members of the public. Moreover, of those who do use the SSN, not all use it as their primary identification number for record-keeping purposes. Of federal respondents, 65 percent use SSN as their primary identifier, while 50 percent of state and 38 percent of county agencies reported doing so. In addition, when agencies do use the SSN as their primary identification number, some agencies also maintain an alternative number that is used in addition to or in lieu of SSNs for certain activities. In fact, at least one-fourth of the respondents across all levels of government said they used SSNs as the primary identifier and also assigned alternative identifiers (38 federal, 30 state, and 25 percent county). There are a number of reasons why agencies use identification numbers other than SSNs. Officials from two county health departments told us that they do not require applicants for the Women, Infant, and Children Program to provide their SSNs because eligibility is determined based on client-provided information.[31] Under these circumstances, program administrators do not need to use SSNs to match data to verify program eligibility. Two officials said that their county health departments use numbers the departments assign as the primary identifier. In such cases, however, health care providers may use SSNs to track patients' medical care across multiple providers or to

[31] However, state auditors in one state told us that when programs do not require an SSN, such as the Women, Infants, and Children Program, it is more difficult to audit the program for compliance because they have to rely on matching data on individuals using name, address, and wage records to ensure that the appropriate people are receiving services. They said this process is time consuming and is not 100 percent accurate. They believe that the use of SSNs for the program would speed up and improve the accuracy of data matches.

coordinate benefit payments. Finally, law enforcement agencies we met with are less likely to consider SSNs as their primary identification number because criminals often have multiple or stolen identities and SSNs.

We asked those agencies that used SSNs as their primary identifier and did not use alternate identification numbers how difficult it would be to change their procedures to permit using different identification numbers in place of SSNs. More than 85 percent of agencies in this category at all levels of government reported that it would be somewhat or very difficult to make this change (93 percent of federal agencies, 93 percent of state agencies, and 87 percent of county agencies). The top four reported reasons why programs might have difficulty making these changes, were (1) that it would prevent interfacing with the computer systems of other departments or programs that use SSNs, (2) it would be too costly, (3) the program's current software would not support the change, and (4) it would require a change in law.

Many Agencies Using SSNs to Administer Programs Do Not Have in Place Uniform Information Security Controls

When government agencies collect and use SSNs as an essential component of their operations, they need to take steps to mitigate the risk of individuals gaining unauthorized access to SSNs or making improper disclosure or use of SSNs. As discussed earlier in this report, agencies at all levels of government use SSNs extensively for a wide range of purposes. Further, they store and use SSNs in varied formats. Over 90 percent of our survey respondents reported using both hard copy and electronic records containing SSNs when conducting their program activities. When using electronic media, many employ personal computers linked to computer networks to store and process the information they collect. This extensive use of SSNs, as well as the various ways in which SSNs are stored and accessed or shared, increase the risks to individuals' privacy and make it both important and challenging for agencies to take steps to safeguard these SSNs.

Uniform guidelines that cut across all levels of government do not exist to specify what actions governments should take to safeguard personal information that includes SSNs. However, certain federal laws lay out a framework for federal agencies to follow when establishing information security programs to protect sensitive personal information, such as

SSNs.[32] The federal framework is consistent with strategies used by those private and public organizations that we previously reported have strong information security programs. [33] The federal framework includes four principles that are important to an overall information security program. These are to periodically assess risk, implement policies and controls to mitigate risks, promote awareness of risks for information security, and continually monitor and evaluate information security practices. To gain a better understanding of whether agencies had in place measures to safeguard SSNs that are consistent with the federal framework, we selected eight commonly used practices found in information security programs—two for each principle. Use of these eight practices could give an indication that an agency has an information security program that follows the federal framework.[34] We surveyed the federal, state, and county programs and agencies on their use of the following eight practices:

Periodically assess risk

- Conduct risk assessments for computer systems that contain SSNs
- Develop written security plan for computer systems that contain SSNs

Implement policies and controls to mitigate risks

- Develop written policies for handling records with SSNs
- Control access to computerized records that contain SSNs, such as assigning different levels of access and using methods to identify employees (e.g., use ID cards, PINS, or passwords)

[32] See federal Government Information Security Reform provisions of the fiscal year 2001 Defense Authorization Act, the federal Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and OMB guidance.

[33] U.S. General Accounting Office, *Executive Guide: Information Security Management, Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998) reported on strategies used by private and public organizations—a financial services corporation, a regional utility, a state university, a retailer, a state agency, a nonbank financial institution, a computer vendor, and an equipment manufacturer—that were recognized as having strong information security programs. The information security strategies discussed in the report were only a part of the organizations' broader information management strategies.

[34] States may also require any number of the eight practices, but the requirements would vary from state to state.

Promote awareness of risks for information security

- Provide employees training or written materials on responsibilities for safeguarding records
- Take disciplinary actions against employees for noncompliance with policies, such as placing employees on probation, terminating employment, or referring to law enforcement

Continually monitor and evaluate information security practices

- Monitor employees' access to computerized records with SSNs, such as tracking browsing and unusual transactions
- Have computer systems independently audited

Responses to our survey indicate that agencies that administer programs at all levels of government are taking some steps to safeguard SSNs; however, potential weaknesses exist at all levels. Many survey respondents reported adopting some of the practices; however, none of the eight practices were uniformly adopted at any level of government. Of the eight practices, the largest percentage of agencies at all three levels of government combined reported controlling access to computerized records that contain SSNs and taking disciplinary actions against employees for noncompliance with policies. The smallest percentage of agencies at all three levels of government combined reported developing written policies for handling records with SSNs and having their information systems security independently audited. Overall, opportunities exist at all levels of government to increase protections against improper access, disclosure, or use of personal information, including SSNs. In general, when compared to state and county government agencies, a higher percentage of federal agencies reported using most of the eight practices.

It is important to note that since 1996 we have consistently identified significant information security weaknesses across the federal government. In early 2002, based on a review of 24 of the largest federal agencies, we reported that federal agencies had not established information security programs consistent with legislative requirements.[35] We found that significant information security weaknesses continued to

[35] U. S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

exist in all major areas for information security programs. For example, (1) risk assessments had not been conducted for all computer systems, (2) polices may have been inadequate or excessive because risks had not been adequately assessed, (3) employees may have been unaware of their security responsibilities because agencies provided little or no training, and (4) effectiveness of security practices was unknown because of inadequate testing and evaluation of security controls. Further, in its February 2001 report to the Congress, OMB noted that many federal agencies have significant deficiencies in every important area of security.[36] Although information security weaknesses may have been reported for certain states and counties, we are not aware of a comparable, comprehensive assessment of information security for either state or county government.

Further, when SSNs are passed from a government agency to another entity, agencies need to take additional steps to continue protections for sensitive personal information that includes SSNs, such as imposing restrictions on the entities to help ensure that the SSNs are safeguarded. OMB guidance specifies a number of requirements federal agencies must follow for certain sharing of personal information.[37] For example, the guidance specifies that federal agencies should prohibit recipient agencies from redisclosing data, except as allowed by law; employ effective security controls; and include mechanisms to hold recipients of data accountable for compliance. The guidance does not prescribe specific steps agencies should take when sharing information containing SSNs and other personal information. Moreover, although state and county governments may establish their own requirements, these would apply only to their respective jurisdiction. In the absence of uniform prescribed steps agencies should take when sharing data, we surveyed agencies on whether they implemented selected requirements when sharing information containing SSNs with outside entities.

As shown in table 5, agency responses indicate that, although most include security requirements in contracts or data sharing agreements, many did

[36] Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform* (Washington, D.C.: February 2002)

[37] OMB Memorandum 01-05 applies to federal data sharing activities covered by the Computer Matching and Privacy Protection Act, as amended. The covered activities are computer-matching for purposes such as verifying program eligibility for federal benefits or recovering delinquent debt. The memorandum states that federal agencies should consider applying the concepts to other data sharing arrangements.

not have a process in place to ensure compliance. Most agencies reported requiring those receiving personal data to restrict access to and disclosure of records containing SSNs to authorized persons and to keep records in secured locations. However, fewer agencies reported having provisions in place to oversee or enforce compliance. For example, only about half of the agencies at all levels of government combined reported using audits to monitor receivers' compliance with requirements. As a result, there is little assurance that entities receiving SSNs from government agencies have upheld their obligation to protect the confidentiality and security of SSNs.

Table 5: Percentage of Program Agencies That Report Imposing Selected Requirements on Outside Entities When Sharing SSNs

	Government agencies sharing SSNs		
Requirement imposed on receivers	**Federal**	**State**	**County**
SSNs must be safeguarded			
Access to SSNs must be restricted to authorized persons	**100%**	**90%**	**84%**
	(33)	(134)	(76)
Disclosure of SSNs must be restricted to authorized persons	**88%**	**92%**	**81%**
	(33)	(135)	(78)
Records with SSNs must be kept in secure location	**97%**	**88%**	**78%**
	(33)	(135)	(78)
Oversight provisions			
Entity must self-report compliance	**34%**	**32%**	**29%**
	(32)	(120)	(76)
Entity must be independently audited for compliance	**59%**	**55%**	**50%**
	(32)	(124)	(76)
Agency imposes penalties for noncompliance	**67%**	**69%**	**50%**
	(30)	(124)	(76)

Legend: The number in parentheses is the number of respondents upon which the percentage is based.

Source: GAO survey of federal, state, and county departments and agencies, using responses from those that reported sharing SSNs. Table includes departments and agencies that administer programs for the public and excludes courts, county recorders, and state licensing agencies.

Efforts are underway at the federal level to more closely review individual federal agencies' security practices. At the direction of the President's Council on Integrity and Efficiency, officials from 15 federal agencies' offices of the inspector general are reviewing their respective agency practices in using and safeguarding SSNs. At the state and county levels, opportunities exist for associations that represent these jurisdictions nationwide to conduct educational programs to highlight the importance

of safeguarding SSNs, encourage agencies to strengthen how they safeguard SSNs, and develop recommended policies and practices for safeguarding SSNs.[38]

Some Agencies Are Beginning to Take Steps to Limit SSN Display on Documents That May Be Viewed by Others

We identified a number of instances where the Congress or governmental entities have taken or are considering action to reduce the presence of SSNs on documents that may be viewed by others who may not have a need to view this personal information. Examples of recent efforts to reduce display follow.

- Treasury relocated the placement of SSNs on Treasury checks to a location that cannot be viewed through the envelope window.
- The Defense Commissary Agency stopped requiring SSNs on checks written by members because of concerns about improper use of the SSNs and identity theft.[39]
- SSA has truncated individuals' SSNs that appear on the approximately 120 million benefits statements it mails each year. At the top of this statement, SSA has included a notice warning individuals to protect their SSNs.
- A state comptroller's office changed its procedures so that it now offers vendors the option of not displaying SSNs on their business permits.
- One state has a statute that prohibits display of SSNs on licenses issued by the state's health department.
- Some states have passed laws prohibiting the use of SSNs as a student identification number.
- Almost all states have modified their policies on placing SSNs on state drivers' licenses. Although it was common practice to find SSNs on

[38] In some cases, where federal agencies administer programs that provide federal funds to states and counties, the federal agency has spelled out program-specific requirements for information security that state and county government agencies are expected to follow when they use federal funds to operate these programs.

[39] As of March 2002, the Navy Exchange System still requires SSNs on checks. Officials told us they hope to implement a system similar to the DOD Commissary by the end of 2002.

licenses only a few years ago, today only ten states routinely display SSNs as a recognizable nine-digit number.[40]

It is important to note that these steps to limit the display of SSNs do not mean the agency has stopped collecting SSNs. In fact, in some cases, the agency may be required by law to collect the SSN but the number need not always be placed on a document or record that is seen by the public.

Agencies are taking these actions even though it is not clear that the SSN displays we identified are, in fact, prohibited. Limitations on disclosing the SSN vary from use to use and among governmental entities. For example, on the federal level, the Privacy Act permits the disclosure of information in a record covered by the act if the agency can show that the use is compatible with the purpose for which it was collected. At the state level, depending on the state and applicable state laws, information about public employees may be considered public information and available upon request. Nonetheless, the efforts to reduce display suggest a growing awareness that SSNs are private information, and the risk to the individual of placing an SSN on a document that others can see may be greater than the benefit to the agency of using the SSN in this manner. However, despite this growing awareness and the actions cited above, many government agencies continue to display SSNs on a variety of documents that can be seen by others.

In addition to the above actions taken by agencies at different levels of government, several bills have been introduced in the Congress that propose to more broadly limit or restrict the display of SSNs by all government entities. For example, some specifically prohibit SSN display on benefit checks or employee identity badges.

Open Nature of Certain Government Records Results in Wide Access to SSNs

Many of the respondents to our survey reported maintaining public records that contain SSNs. Many of these records are maintained by county clerks or recorders and certain state agencies. In addition, courts at all three levels of government maintain records that contain SSNs and are available to the public. Some of the documents in these records that contain SSNs are created by the governmental entity itself, while others

[40] SSNs are displayed on all licenses in one state, on all licenses except where the driver has asked that they be omitted in nine states, and only on licenses requested by the driver in 14 states.

are submitted by members of the public, attorneys, or financial institutions. The public has traditionally gained access to these public records by visiting the offices where they are maintained and requesting certain documents or by browsing among hard copies or microfilm to find the desired information. This has served, at least in part, as a practical deterrent to the widespread collection and use of others' SSNs from public records. However, the growth of electronic record keeping has enabled a few agencies to provide or even sell their data in bulk. Moreover, although few entities report making SSNs available on the Internet, several officials told us they are considering expanding the volume and type of public records available on their Web site.

Many State and County Public Records Contain SSNs

As shown in table 6, all of the federal courts and over two-thirds of the state and county courts, county recorders, and state licensing agencies that reported maintaining public records indicated that these records contained SSNs. In addition, some program agencies also reported maintaining public records that contain SSNs. (For more information on the types of federal programs and state and county agencies that reported maintaining public records, see app. III).

Table 6: Of Courts, County Recorders, and State Licensing Agencies; and of Program Agencies That Maintain Public Records, Percentage That Maintain Public Records That Contain SSNs

	Federal	State	County
Courts, recorders, and licensing agencies that maintain public records with SSNs	**100%**	**68%**	**77%**
	(3)[a]	(31)	(95)
Program agencies that maintain public records with SSNs	**23%**	**29%**	**33%**
	(22)	(189)	(140)

[a]All three respondents were from federal courts.

Legend: The number in parentheses is the number of respondents upon which the percentage is based.

Source: Data from GAO survey of federal, state, and county departments and agencies.

County clerks or recorders (hereinafter referred to as recorders) and certain state agencies often maintain records that contain SSNs because these offices have traditionally been the repository for key information that, among other things, chronicles various life events and other activities

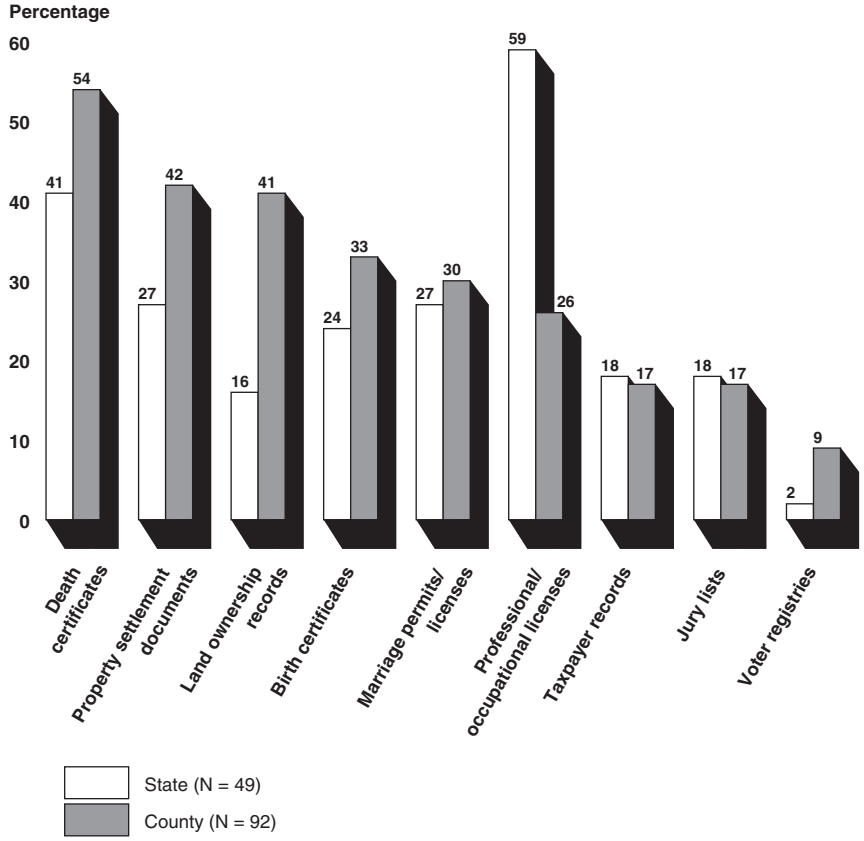
of individuals as they interface with government.[41] For example, they often maintain records on an individual's birth, marriage, and death. They maintain documentation that an individual has been licensed to work in certain professions, such as medical, legal, and public accounting. In addition, they may maintain documentation on certain transactions, such as property ownership and title transfer. This is done, according to recorders we met with, to make ownership known and detect any liens on a parcel of land before making a purchase.

SSNs appear in these public records for a number of reasons. They may already be a part of a document that is submitted to a recorder for official preservation. For example, military veterans are encouraged to file their discharge papers with their local recorder's office to establish a readily available record of their military service, and these documents contain the SSN because that number is the individual's military identification number.[42] Also, documents that record financial transactions, such as tax liens and property settlements, contain SSNs to help identify the correct individual. In other cases, government officials are required by law to collect SSNs. For example, to aid in locating noncustodial parents who are delinquent in their child support payments, the federal Personal Responsibility and Work Opportunity Reconciliation Act of 1996 requires that states have laws in effect to collect SSNs on applications for marriage, professional, and occupational licenses. Moreover, some state laws allow government entities to collect SSNs on voter registries to help avoid duplicate registrations. Again, although the law requires public entities to collect the SSN as part of these activities, this does not necessarily mean that the SSNs always must be placed on the document that becomes part of the public record. Figure 3 shows the percentage of state and county entities that display SSNs on each of the types of public records listed.

[41] It varies from state to state as to whether certain records, such as marriage licenses and birth certificates, are maintained in county or state offices. Certain documents, however, such as land and title transfers, are almost always maintained at the local, or county, level.

[42] Veterans are advised that these are important documents, which can be registered/recorded in most states or localities for a nominal fee making retrieval easy. In October 2001, DOD added a cautionary statement that recording these documents could subject them to public access in some states or localities.

Figure 3: Percentage of State and County Entities that Display SSNs on Each of the Types of Public Records Listed



Legend: N is the number of respondents upon which the percentage is based.

Source: GAO surveys of state and county government agencies, using responses from those that reported maintaining at least one of the above listed public records containing SSNs.

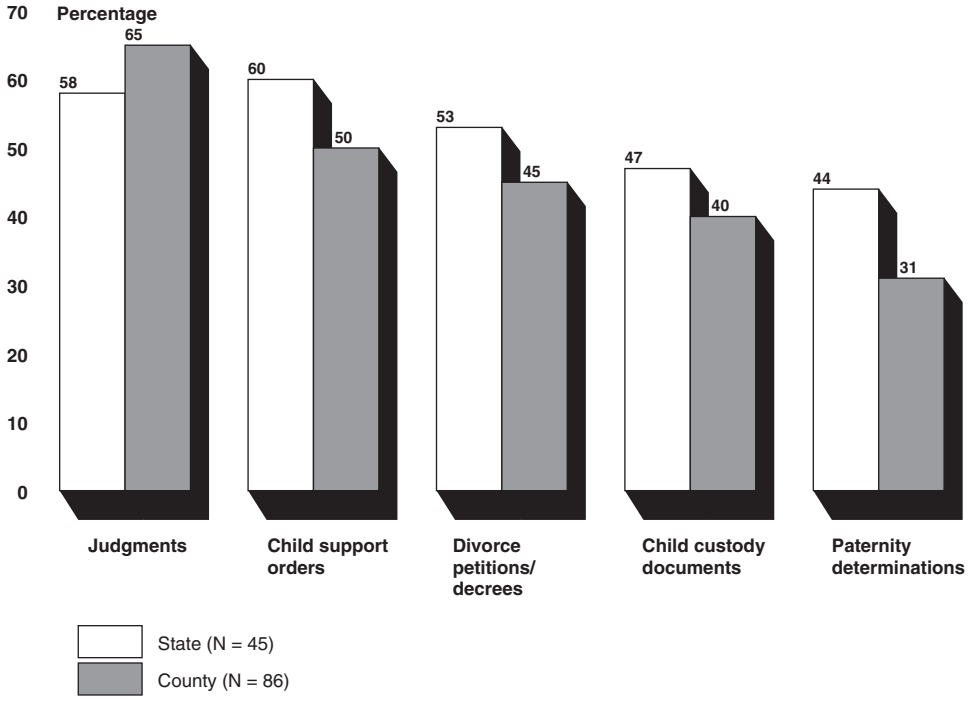
Courts at all three levels of government also collect and maintain records that are routinely made available to the public. Court records overall are presumed to be public; however, each court may have its own rules or practices governing the release of information.[43] The rationale for making these records public is that keeping court activities open helps ensure that

[43] In some states, for example, adoption records, grand jury records, and juvenile court records are not part of the public record. In addition, some court documents pertinent to the cases may or may not be in the public record, depending on local court practice. Finally, the judge can choose to explicitly seal a record to protect the information it contains from public review.

justice is administered fairly. In addition, the legal requirement that bankruptcy court documents remain open for public inspection is to ensure that bankruptcy proceedings take place in a public forum to best serve the rights of both creditors and debtors.

As with recorders, SSNs appear in court documents for a variety of reasons. In many cases, SSNs are already a part of documents that are submitted by attorneys or individuals. These documents could be submitted as part of the evidence for a proceeding or could be included as part of a petition for an action, such as a judgment or a divorce. In other cases, courts include SSNs on documents they and other government officials create, such as criminal summonses, arrest warrants, and judgments, to increase the likelihood that the correct individual is affected (i.e., to avoid arresting the wrong John Smith). In some cases federal law requires that SSNs be placed in certain records that courts maintain. For example, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 requires that SSNs be placed in records that pertain to child support orders, divorce decrees, and paternity determinations. Again, this assists child support enforcement agencies in efforts to help parents collect money that is owed to them. These documents may also be maintained at county clerk or recorders' offices. Figure 4 shows percentage of state and county entities that display SSNs on each of the types of public records listed.

Figure 4: Percentage of State and County Entities that Display SSNs on Each of the Types of Public Records Listed



Legend: N is the number of respondents upon which the percentage is based.

Source: GAO survey of state and county government agencies, using responses from state county courts and county recorders that report maintaining at least one of the above listed records containing SSNs.

When federal, state, or county entities, including courts, maintain public records, they are generally prohibited from altering the formal documents. Officials told us that their primary responsibility is to preserve the integrity of the record rather than protecting the privacy of the individual named in the record. Officials told us they believe they have no choice but to accept the documents with the SSNs and fulfill the responsibility of their office by making them available to the general public.

Traditional Access to Public Records Has Practical Limitations That Would Not Exist on the Internet

Traditionally, the public has been able to gain access to SSNs contained in public records by visiting the recorder's office, state office, or court house; however, the requirement to visit a physical location and request or search for information on a case-by-case basis offers some measure of protection against the widespread collection and use of others' SSNs from public records.[44] Depending on the local practice, a member of the public may request specific documents from a clerk or may be able to browse through thousands of hard copies of documents, often dating back many decades or more. In addition, some counties make available documents that have been microfilmed or microfiched. Under these circumstances, it may be somewhat easier to find information on individuals; however, the information available would be limited to the type of record that is microfilmed (e.g., property settlement documents). In other words, the effort involved in obtaining documents by visiting local offices in effect helps insulate individuals from possible harm that could result from SSN misuse because of the time and effort required. A county recorder told us that the individuals willing to expend the time and effort to visit local offices to review public records generally have a business need to do so.

However, this limited access to information in public records is not always the case. We found examples where members of the public can obtain easy access to larger volumes of documents containing SSNs. Some offices that maintain public records offer computer terminals set up where individuals can look up electronic files from a site-specific database. In one of the offices we visited, documents containing SSNs that are otherwise accessible to the public are also made available in bulk to certain groups. In one county we visited, title companies have an arrangement to scan court documents to add to their own databases before the documents are filed in the county recorder's office.

When comparing the sharing practices of courts, state licensing agencies, and county recorders to program agencies that collect and use SSNs, a higher percentage of county recorders reported sharing information containing SSNs with credit bureaus, researchers, debt collection agencies, private investigators, and marketing companies. When courts, state licensing agencies, or county recorders share public records containing SSNs, they do not restrict receivers' use or disclosure of the data.

[44] Some jurisdictions also permit citizens to request public records through the mail.

Government offices may charge fees when providing copies of records in various formats that may contain SSNs and other personal information. More than 20 percent of county agencies and 25 percent of state agencies reported charging fees when providing SSNs to a contractor, researcher, individual, or other entity during the last 12 months.[45] In most cases, the fees only covered costs for providing the information. However, 13 percent of the state respondents and 44 percent of the county respondents that charged fees reported making a profit from charging a fee. At the state level, the smallest profit reported from this sale of records over the last 12 months was $5,000, and the largest was $2,068,400. On the county level, the smallest profit reported over the same period was $200, and the largest was more than $2 million. The range in revenue may be partially explained by the fact that officials from these agencies may sell these records to individuals requesting one or a small number of documents, or they may sell these records in bulk. For example, one state sells its unclaimed property database, which often contains SSNs.

Finally, few agencies reported that they place SSNs on their Internet sites; however, this practice may be growing. Of those agencies that reported having public records containing SSNs, only 3 percent of the state respondents and 9 percent of the county respondents reported that the public can access these documents on their Web site. In some cases, such as the federal courts, documents containing SSNs are available on the Internet only to paid subscribers. In other cases, large numbers of SSNs may be available to the general public. For example, one state's Office of the Comptroller of Public Accounts displays SSNs of business owners on their public web site embedded in Vendor/Taxpayer Identification Numbers. Moreover, increasing numbers of departments are moving toward placing more information on the Internet. We spoke with several officials that described their goals for having records available electronically within the next few years. Providing this easy access of records potentially could increase the opportunity to obtain records that contain SSNs that otherwise would not have been obtained by visiting the government agency.

[45] Our surveys were mailed first in August 2001, and the last surveys analyzed were received in March 2002.

Some Governments and Agencies Are Taking Innovative Actions to Limit Use and Display of SSNS in Public Records

When SSNs are found in public records, some government entities are trying to strike a new balance between their responsibility to allow the general public access to documents that have traditionally been made available for public review and an increased interest in protecting the privacy of individuals. This is possible primarily for those records the agency or court creates. In these cases, the government entity may still collect SSNs, which may be required by law or important for record-keeping purposes, but the number itself need not be displayed. For those records and documents submitted by others, it is more difficult to exclude the SSN unless the individual or business preparing the document omits it before submission.

Alternatives to Displaying SSNs in Public Records Exist

When government agencies create public documents or records, such as marriage licenses, some are trying new innovative approaches that protect SSNs from public display. Some agencies have developed alternative types of forms to keep SSNs and other personal information separate from the portion of a document that is accessible to the general public. In these cases, even if the government agency is required by law to record the SSN, the number does not always need to be displayed on the copy of the document that is made available to the public.[46] Changing how the information is captured on the form can help solve the dilemma of many county recorders who, because they are the official record keepers of the county, are usually not allowed to alter an original document after it is officially filed in their office. For example, a county recorder told us that Virginia recently changed its three part marriage application and license form. Currently, only one copy of the form is routinely made available to the general public and that copy does not contain the SSN while the other two copies do contain the SSN. However, a county recorder told us that even this seemingly simple change in the format of a document can be challenging because, in some cases, the forms used for certain transactions are prescribed by the state.

In addition to these efforts at recorders offices, courts at all three levels of government have made efforts to protect SSNs in documents that the general public can access through court clerk offices. For example, one state court offers the option of filing a separate form containing the SSN

[46] In other cases, the law requires that the SSN appear on the document itself, as on death certificates.

that is then kept separate from the part of the record that is available for public inspection.

These solutions, however, are most effective when the recorder's office, state agencies, and courts prepare the documents themselves. In those many instances where others file the documents, such as individuals, attorneys, or financial institutions, the receiving agency has less control over what is contained in the document and, in many cases, must accept it as submitted. Officials told us that, in these cases, educating the individuals who submit the documents for the record may be the most effective way to reduce the appearance of SSNs. Such educational efforts could begin with informing individuals who submit documents to these offices that, once submitted, anything in that document is open to the public for review.[47] For example, one individual who submitted his military discharge papers to his county recorder's office expressed concern about having done so after he found out that his document was available for anyone to review. Several officials suggested placing signs in offices where public records are maintained. Others suggested finding additional ways to notify the public of the nature of public records and the consequences of submitting documents with SSNs on them.[48] In addition, financial institutions, title companies, and attorneys submit a large portion of the documents that become part of the public record in recorder's offices and the courts. These entities could begin to consider whether SSNs are required on the documents they submit. It may be possible to limit the display of SSNs on some of these documents or, where SSNs are deemed necessary to help identify the subject of the documents, it may be possible to truncate the SSN to the last four digits.

Redacting SSNs from Existing Records Can Be Difficult

While the above options are available for public records created after an office institutes changes, fewer options exist to limit the availability of SSNs in records that have already been officially filed or created. One option is redacting or removing SSNs from documents before they are made available to the general public. In our fieldwork, we found instances

[47] In these cases when the governmental office is not requesting that the individual disclose his or her SSN, the receiving office is not required to provide the individual with the information required under section 7 of the Privacy Act.

[48] There are few appropriate vehicles available to notify large segments of the public of this type of information. SSA has a public education campaign and also sends a statement of earnings and projected benefits to about 123 million people each year.

where departments redact SSNs from copies of documents that are made available to the general public, but these tended to be situations where the volume of records and number of requests were minimal, such as in a small county. Most other officials told us redaction was not a practical alternative for public records their offices maintain. Although redaction would reduce the likelihood of SSNs being released to the general public, we were told it is time-consuming, labor intensive, difficult, and in some cases would require change in law. In documents filed by others outside of the office, SSNs do not appear in a uniform place and could appear many times throughout a document. In these cases, it is particularly labor-intensive and a lengthy process to find and redact SSNs.

In addition, especially in large offices that receive hundreds of requests for general public documents per day, we were told redacting SSNs from each document before giving it to a member of the general public would require significant staff resources. In one large urban county, the district clerk's office sells about 930,000 certified pages a year from family law cases. The district clerk estimates that it would cost his office an additional $1 million per year in staff time and related expenses to redact SSNs from all of those documents before they are made available to the general public.

Moreover, redaction would be less effective in those offices where members of the general public can inspect and copy large numbers of documents without supervision from office staff. In these situations, officials told us that they could change their procedures for documents that they collect in the future, but it would be extremely difficult and expensive to redact SSNs on documents that have already been collected and filed. In several of these offices we visited, documents are available in hard copy, on microfilm, on microfiche, or in electronic format. Copies of thousands of documents, often dating back many decades or more, are kept in large rooms where anyone can browse through them. In addition, some counties have computer terminals set up where individuals can look up electronic files on their own. In these cases, the only way to prevent disclosure of SSNs would be to redact them from all of the past records, which officials told us would be extraordinarily costly and in some cases (e.g., on microfiche and electronically scanned documents) would be extremely difficult.

Some of the bills currently before the Congress call for redacting SSNs from public records or otherwise ensuring that the public does not have access to the numbers. In some cases, the proposals would apply to all SSN displays originally occurring after 3 years from the date of their enactment. In other cases, the proposal calls for redacting all SSNs that

are routinely placed in a consistent and predictable manner on a public record by the government entity, but it would not require redacting SSNs that are found in varying places throughout the record.

Agencies Are Considering Limiting Information Placed on the Internet

To protect SSNs that the general public can access on the Internet, some courts and government agencies are examining their policies to decide whether SSNs should be made available on documents on their Web sites. In our fieldwork, we heard many discussions of this issue, which is particularly problematic for courts and recorders, who have a responsibility to make large volumes of documents accessible to the general public. On the one hand, officials told us placing their records on the Internet would simply facilitate the general public's ability to access the information. Furthermore, officials expressed concern that placing documents on the Internet would remove the natural deterrent of having to travel to the courthouse or recorder's office to obtain personal information on individuals.

Again, we found examples where government entities are searching for ways to strike a balance. For example, the Judicial Conference of the United States recently released a statement on electronic case file availability and Internet use in federal courts. They recommended that documents in civil cases and bankruptcy cases should be made available electronically, but SSNs contained in the documents should be truncated to the last four digits. Also, we spoke to one county recorder's office that had recently put many of its documents on their web site, but had decided not to include categories of documents that were known to contain SSNs. In addition, some states are taking action to limit the display of SSNs on the Internet. Laws in Arizona and Rhode Island prohibit the display of students' SSNs on the Internet. Even though the incidence of SSNs on government Web sites is minimal right now, some officials told us they were considering or were in the process of making more documents available on the Internet. Without some kind of forethought about the inherent risk posed by making SSNs and other personal information available on the Internet, it is possible that SSNs will become increasingly available to the general public via the Internet.

Statewide Efforts Have Had Far-Reaching Effects

The examples of efforts to limit the disclosure of SSNs cited above stem from initiatives taken by certain offices within states or from state laws that restrict specific types of SSN uses. By their nature, these efforts are limited only to the specific offices or types of use. However, efforts to protect individuals' privacy can be more far-reaching when the initiatives

are statewide. For example, in April 2000, the governor of Washington signed an executive order intended to strengthen privacy protections for personal information held by state agencies on the citizens, as well as ensure that state agencies comply fully with state public disclosure and open government laws. Under Washington's executive order, state agencies are required to protect personal information to the maximum extent possible by (1) minimizing the collection, retention, and release of personal information by the state,(2) prohibiting the unauthorized sale of citizens' personal information by state government, and (3) making certain that businesses that contract with the state use personal information only for the contract purposes and cannot keep or sell the information for other purposes.

A number of actions to limit SSN use and display resulted from this order. In response to the executive order, state agencies across Washington reviewed their forms and documents on which SSNs appeared and identified displays that were deemed unnecessary, that is, displays where the appearance of the SSN on the document was not deemed vital to the business of the agency. In these cases, agency officials removed the SSNs from the forms or documents. For example, the state Department of Natural Resources removed SSNs from employee performance evaluation notices and worklists, individual employee training profiles, and employee exit questionnaire forms. Officials told us that they have also discontinued requiring SSNs on leave requests, travel reimbursements, and training forms. The Washington Office of the Attorney General deleted SSNs from training and attendance forms, personnel questionnaires, employee separation forms, flexiplace work schedule forms, and others. In addition, the Washington Department of Labor and Industries separated information in personnel files that may be reviewed by supervisors from payroll documents. In addition, private information, such as SSNs, is being redacted from employee documents that can be viewed by others, and applicants for jobs in a county we visited are not required to provide their SSN until they are offered a job.

Washington agencies also changed the format of certain public records to limit the disclosure of SSNs. For example, the SSN and other personal information are only included on the back of the marriage certificate form, which is not supposed to be copied or given to the general public. In certain Washington courts, SSNs and other personal information required in family law cases must be written on a separate form from the rest of the court document, and this form is then kept in a restricted access file. This means that the public does not have access to the information, and internal access is limited to judges, commissioners, other court personnel,

and certain state administrative agencies that administer family law programs. Anyone else requesting access to these case records must petition the court and make a showing of good cause as to why access should be granted.

Agencies for Washington state also reviewed and certified all contracts involving data sharing as having appropriate requirements to prevent and detect contractors' unauthorized SSN use. In fact, we were told of one case where the Washington state Department of Licensing monitored a contractor's compliance with maintaining the privacy of personal information by, in part, providing the contractor with certain easily identifiable information that other entities did not have. By tracing the flow if this information, officials discovered that the contractor had improperly disclosed personal information and terminated the contract.

Minnesota is another example of a state where action on the state level, in this case in the form of a law, has made a difference in how SSNs are treated in public records. The Minnesota Government Data Practices Act, which predates the federal Privacy Act, regulates the handling of all government data that are created, collected, received, or released by a state entity, political subdivision, or statewide system, no matter what form the data are in, or how they are stored or used. Referred to as the nation's first privacy act, Minnesota's statute regulates what information can be collected, who can see or have copies of the information, and civil penalties for violation of the act. Minnesota uses a detailed approach to classifying data as not public. One statutory provision specifically classifies SSNs collected by state and local government agencies as not public. As a result of this law, individuals must be informed either orally or in writing of their privacy rights whenever the state collects sensitive information about them. In addition, individuals filing a civil court document can either put their personal information on a separate form or submit two copies of the document, only one of which contains SSNs. The information containing SSNs is then filed separately from the rest of the court document and is not open to the general public.

Neither state tracked costs for making changes to better protect personal information, such as SSNs. Generally, state officials reported that the costs for implementing the initiative in Washington and carrying out the state statute in Minnesota are absorbed in the cost of the states' overall operations.

Conclusions

SSNs are widely used in all levels of government and play a central role in how government entities conduct their business. As unique identifiers, SSNs are used to help make record keeping more efficient and are most useful when government entities share information about individuals with others outside their organization. The various benefits from sharing data help ensure that government agencies fulfill their mission and meet their obligation to the taxpayer by, for example, making sure that the programs serve only those eligible for services.

However, as governments enjoy the benefits from using SSNs, they are not consistently safeguarding this personal information. They are not consistently providing individuals with required information about how their numbers will be used, thus depriving SSN holders of the basis to make a fully informed decision about whether to provide their SSN. Nor do governments have in place uniform information systems security measures. This suggests that these numbers and other sensitive information are at risk for improper disclosure and that more can be done to implement practices to help protect them. Further, when government agencies display the SSN on documents, such as employee identification badges and benefit eligibility cards, that are viewed by others who may not have a need for this personal information, the agency displaying the SSN increases the risk that the number may be improperly obtained and misused. In some cases, the risk for misuse may outweigh any benefit of its display.

Safeguarding SSNs in public records offers an even greater challenge because of the inherent tension between the nature of public records, that is, the need for transparency in government activities, and the need to protect individuals' privacy. Plans to bring public records on-line and make them available over the Internet add urgency to this issue. Although the on-line access to such records will greatly increase convenience for those members of the public who use them, personal information like SSNs that is contained in some of these records will also be made readily available to the public. Addressing the issues of whether the traditional rules of public access should apply to electronic records, particularly those found on the Internet, is both urgent and vital. Without policies specifying ways to safeguard SSNs on the Internet, the potential for compromising individuals' privacy and the potential for SSN misuse will increase significantly.

Further, although improving safeguards for government use of SSNs and other personal information is important, even the most successful efforts by government agencies cannot eliminate the risk to individuals that their

SSNs will be misused because SSNs are so widely used in the private sector as well. Any effort to significantly reduce the risk of improper disclosure and misuse of SSNs would require added safeguards and limits on private sector use and display of the SSN as well. Nonetheless, measures to protect privacy by public sector entities could at least help minimize the risk of misuse.

Under current law, weaknesses in the safeguards applied to SSNs can be more readily addressed in the federal government than in the state and local governments. Federal laws lay out a framework for information systems security programs to help protect sensitive information overall. More specific to the SSN, the Privacy Act places broad restrictions on federal government use and disclosure of personal information such as the SSN. Improved federal implementation of these requirements can be accomplished within current law.

On the state and local level, the Privacy Act does have a provision that applies to state and local governments albeit more limited than the requirements on the federal government. This requirement—that all levels of government provide certain information to SSN holders, such as how their SSNs will be used—is not consistently applied. However, strengthening enforcement of this provision of the act, while important, will not address the more basic protection issues related to information security and public display. Doing so by mandating stronger state and local government safeguards for such personal information as the SSN, however, confronts questions of jurisdiction and policy that are beyond the scope of this report. Nonetheless, such questions should be addressed quickly, before public sector information is compromised and before public records become fully electronic. Accordingly, we are making recommendations to OMB to help strengthen safeguards in federal agencies, and we are presenting a matter for congressional consideration to facilitate intergovernmental collaboration in strengthening safeguards at the state and local levels.

Recommendations

The Privacy Act and other federal laws prescribe actions federal departments and agencies must take to assure the security of SSNs and other personal information. Because these requirements may not be uniformly observed, we recommend that the administrator, Office of Information and Regulatory Affairs, OMB, direct federal agencies to review their practices for securing SSNs and providing required information. As part of this effort, agencies should also review their practices for displaying SSNs.

To better inform state and local governments of their responsibilities under section 7 of the Privacy Act, we recommend that the administrator, Office of Information and Regulatory Affairs, OMB, direct his staff to augment the Privacy Act guidance by specifically noting that section 7 applies to all federal, state and local government agencies that request SSNs, or take other appropriate steps.

Matter For Congressional Consideration

To address SSN security and display issues in state and local government and in public records, including those maintained by the judicial branch of government at all levels, the Congress may wish to convene, in consultation with the president, a representative group of federal, state and local officials including, for example, state attorneys general, county recorders, and state and local chief information officers, selected members of the Congress, and state or local elected officials, to develop a unified approach to safeguarding SSNs used in all levels of government and particularly those displayed in public records. This approach could include recommendations for congressional consideration. GAO could assist in identifying representative participants and in convening the group.

Agency Comments

We requested comments on a draft of this report from the director of OMB and the commissioner of SSA or their designees. We also requested that other officials review the technical accuracy of their respective agency or entity activities discussed in the draft, and we incorporated their changes where appropriate.

SSA officials informed us that they would not provide written comments on the draft because the report does not make recommendations to the agency and comments were not required. However, we were told that the deputy commissioner shares the concerns expressed in the report and agrees with the conclusions.

We did not receive written comments from the OMB director; however, other OMB officials provided us oral comments on the draft. They generally agreed with our recommendation that OMB direct federal agencies to review their practices for securing SSNs and providing the required information. In regard to our recommendation that OMB augment Privacy Act guidance or take other appropriate steps to better inform state and local governments of their responsibilities under section 7 of the Act, OMB officials told us that they are unsure of the need for additional OMB guidance in this area. They indicated that guidance on section 7 already

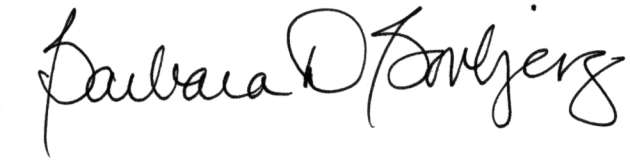
exists in a publicly-available format on the Justice Department's Web site. In addition, they believe the section 7 provision is quite short and appears to be fairly self-explanatory. As the guidance in the Justice Web site indicates, some interpretive issues have arisen in litigation; however, OMB officials said the Justice guidance readily explains those issues. In addition, they said, the report does not indicate substantive areas where additional interpretive guidance is needed. However, they noted that the report does suggest that state and local officials may not be aware of section 7 provisions. In that case, they said increasing awareness of these legal requirements may warrant further consideration. Accordingly, OMB plans to consider, in consultation with other federal agencies, options for increasing state and local officials' awareness on this subject.

Although OMB correctly points out that the overview of the Privacy Act on the Department of Justice Web site refers to the requirements of section 7, we believe our finding that a significant percentage of state and local agencies reported they do not routinely provide individuals with the information required under section 7 supports the need for additional action. We agree that state and local officials may not be aware of section 7 requirements, and we believe there is a need to increase the awareness both of state and local officials administering the programs and of those monitoring compliance at the state and local levels. Because OMB is the federal agency responsible for assisting with and overseeing the implementation of the Privacy Act, we believe it should take the lead on increasing state and local awareness of section 7. However, we recognize that OMB's role with respect to state and local governments is limited and support the agency's idea to act in consultation with other federal agencies to take other steps it deems appropriate to accomplish this increased awareness.

We are sending copies of this report to the Honorable Jo Anne B. Barnhart, commissioner of SSA, Mr. Mitchell E. Daniels Jr., the director of OMB, and others who are interested. Copies will also be made available to others upon request.

If you or your staff have any questions concerning this report, please call me on (202) 512-7215. The major contributors to this report are listed in appendix IV.

Sincerely yours,



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

Appendix I: Scope and Methodology

To complete the objectives for this assignment, we used a combination of in-depth interviews, site visits, and mail surveys. To gain a preliminary understanding of how governments use and protect SSNs and to help design our survey and site-visit questions, we met with a number of government agencies, associations, and privacy experts. At the federal level, we interviewed officials from OMB, the Office of Personnel Management, SSA, and the FTC. At the state level, we interviewed officials from the National Governors Association, the National Association of State Auditors, Comptrollers, and Treasurers, the American Association of Motor Vehicle Administrators, the National Conference of State Legislatures, and the National Association of State Chief Information Officers, which represents state chief information officers, and the state of Maryland. At the county level, we interviewed officials from the National Association of County Election Officials, Clerks, and Recorders, the National Association of Counties, and Fairfax and Fauquier Counties, Virginia. We also met with or contacted officials/organizations regarded as experts in the privacy area, which included a privacy consultant and an official from the Privacy Journal. In addition, we reviewed published reports and studies on SSN use and privacy issues.

To gain an understanding of the requirements for both using and protecting SSNs, we reviewed pertinent federal legislation, federal guidance and directives regarding the use and handling of SSNs and other personal information, GAO reports, and various studies of state SSN use and privacy laws. To develop our criteria for assessing the actions government agencies take to protect SSNs, we drew from applicable federal laws, primarily the Government Information Security Reform provisions of the Fiscal Year 2001 Defense Authorization Act, OMB Circular A-130 and other guidance, and the Federal Information System Controls Audit Manual that specifies guidelines for federal agencies to safeguard sensitive information stored in computer systems. We also drew from our work on best practices used by private companies and public sector organizations identified in our *Executive Guide: Information Security Management, Learning From Leading Organizations*.[1] Finally, we held a 1-day seminar on innovative practices used by the private sector to protect sensitive information. Attendees included officials from the Private Sector Council and member firms, including Kaiser Permanente, a health care provider; State Street Bank, a large commercial bank; and Allstate, an insurance company.

[1] GAO/AIMD-98-68.

Our surveys, site visits, and in depth interviews with officials of targeted federal, state, and county programs focused on the following areas: how SSNs are used (for both programmatic and personnel-related purposes), how and why SSNs are shared with other entities (including contractors), what information programs provide individuals when agencies collect and use their SSNs, how agencies maintain and safeguard SSNs and other personal data, and the cost for minimizing use or implementing alternatives to using SSNs.

At the federal level, we surveyed all 14 cabinet-level agencies plus the Environmental Protection Agency, the Small Business Administration, SSA, and the federal court system. The latter three agencies and the federal court system were added for breadth of coverage to ensure that we covered regulatory agencies, independent agencies, and courts.[2] We asked that each agency identify the five programs that maintain documents containing the SSNs of the largest number of individuals and then asked representatives of those programs to complete a questionnaire. To the extent that an agency had a program whose primary purpose was to conduct research that used records with individuals' SSNs as part of that research, we asked that it be substituted for one of the five programs. Finally, we distributed a different survey to agency personnel offices to determine how agencies used and protected the SSNs of their employees. The federal agency and the federal personnel questionnaires were each pretested at least twice. Because we don't know how many programs within the federal agencies we surveyed maintain records containing individuals' SSNs, we cannot calculate a response rate for the federal agency questionnaire. In total, 58 federal programs, agencies, or courts returned a completed questionnaire. Of the 18 federal agencies to which we sent a questionnaire, 15 returned a completed questionnaire for at least one program. We now know that one of the 18 agencies that received a questionnaire did not have any programs that maintained records containing SSNs. In addition, 18 federal personnel offices received our personnel questionnaire, and of those 15 returned completed questionnaires, for a response rate of 83 percent.

At the state level, our work covered all 50 states and the District of Columbia. In each state, we distributed the surveys to seven preselected

[2] Although the IRS uses and shares SSNs with a number of governmental entities, we did not focus on the requirements for the use and dissemination of taxpayer information because they are distinct from many of the requirements covered in this report. See GGD-99-164.

programs or functions that were identified by others as likely to be ones that maintained documents containing the SSNs of the largest number of individuals. These included the departments of (1) human services, (2) health services and vital statistics, (3) education, (4) labor and licensing, (5) judiciary, (6) public safety and corrections, and (7) law enforcement.[3] Finally, we also surveyed each state's personnel office. The state department and personnel questionnaires were each pretested twice. In total, 424 state programs or functions were mailed a questionnaire, and of those 307 returned completed questionnaires, for a response rate of 72 percent. In addition, of the 51 state personnel offices that were mailed our state personnel questionnaire, 42 completed and returned it, for a response rate of 82 percent.

At the local level, we selected 90 counties with the largest populations in the nation as our focus. Our goal was to choose areas with large numbers of persons that would be affected by the way local government agencies handled SSNs. We again focused on those preselected programs or functions that county officials reported as ones that maintained documents containing the SSNs of the largest number of individuals. These are, in general, the same programs or functions that we focused on in the states; we also surveyed the county clerk or recorder, which was identified as a place that maintained a large number of records containing individuals' SSNs. Finally, we surveyed each county's personnel office. The county department and personnel questionnaires were each pretested twice. In total, 488 county programs or functions were mailed a questionnaire, and of those 344 returned completed questionnaires, for a response rate of 70 percent. In addition, 90 county personnel offices were mailed our county personnel questionnaire, and of those 64 completed and returned it, for a response rate of 71 percent.

In-depth interviews and site visits to federal agencies, states, and counties were used to supplement the survey data by providing more detailed information on the uses of SSNs, reasons for their use, and challenges encountered in protecting them. Interviews and site visits for federal programs were selected based on breadth of coverage, novel or innovative steps to protect SSNs, and special interest by the requestors. We

[3] We did not target state Departments of Motor Vehicles; instead we incorporated information gathered by another GAO team studying SSN use in these state agencies for child support enforcement efforts. See GAO-02-239. In addition, we did not focus on state tax agencies because the requirements for sharing taxpayer information are distinct from the other requirements in this report.

conducted in-depth interviews with officials from the (1) Federal Court System - Administrative Office of the U.S. Courts; (2) Centers for Medicare and Medicaid Services; (3) Department of Education's Student Financial Assistance; (4) Department of Housing and Urban Development's Low Income Housing Programs; (5) DOD Commissaries; and (6) the U.S. Marshals Service. At the state level, we conducted site visits to the states of Texas, Washington, and Minnesota. We selected these states because their legal framework and practices regarding the openness of government records and the privacy of individuals varied. Texas has a strong open records tradition; Washington state has an executive order in place that has serves to limit the availability of certain personal information; and Minnesota has a privacy law that also serves to limit the availability of certain types of information. At the county level, we conducted site visits to Harris County, Texas; King County, Washington; and Aitkin County in Minnesota.[4] We visited counties located in states we selected for site visits to help us understand how state policy affects local practices. Also, we selected Aitkin County, Minnesota to gain the perspectives of a smaller rural county. During our site visits, we met with officials from the departments or agencies that were considered heavy users of SSNs. We also met on two occasions with a group of county clerks and recorders from urban and smaller rural counties.

To provide information on the role of government use of SSNs in identity theft, we incorporated information provided by GAO's Tax Administration and Justice group, which was obtained as part of a broader effort to describe the prevalence and cost of identity theft.[5] The information we used from that effort is based on interviews with and documentation provided by the FTC, SSA's Office of Inspector General, IRS, Federal Bureau of Investigation, U.S. Secret Service, and credit bureaus among others.

We performed our work at SSA headquarters in Baltimore, Maryland; at Maryland state offices in Annapolis, Maryland; Washington D.C.; and at selected locations including Austin, Texas; Harris County, Texas; Olympia, Washington; King County, Washington; St. Paul Minnesota; and Aitkin County Minnesota. We conducted our work between February 2001 and

[4] We also visited court officials at Anoka County, Minnesota.

[5] U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington D.C.: Mar. 1, 2002).

March 2002 in accordance with generally accepted government auditing standards.

Appendix II: Federal Laws That Restrict SSN Disclosure

The following federal laws establish a framework for restricting SSN disclosure:

The Freedom of Information Act (FOIA) (5 U.S.C. 552) – This act establishes a presumption that records in the possession of agencies and departments of the executive branch of the federal government are accessible to the people. FOIA, as amended, provides that the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the federal government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to state and local governments.

The Privacy Act of 1974 (5 U.S.C. 552a) – The act regulates federal government agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records.[1] The act prohibits the disclosure of any record contained in a system of records unless the disclosure is made on the basis of a written request or prior written consent of the person to whom the records pertains, or is otherwise authorized by law. The act authorizes 12 exceptions under which an agency may disclose information in its records. However, these provisions do not apply to state and local governments, and state law varies widely regarding disclosure of personal information in state government agencies' control. There is one section of the Privacy Act, section 7, that does apply to state and local governments. Section 7 makes it unlawful for federal, state, and local agencies to deny an individual a right or benefit provided by law because of the individual's refusal to disclose his SSN. This provision does not apply (1) where federal law mandates disclosure of individuals' SSNs or (2) where a law existed prior to January 1, 1975 requiring disclosure of SSNs, for purposes of verifying the identity of individuals, to federal, state or local agencies maintaining a system of records existing and operating before that date. Section 7 also requires federal, state and local agencies, when requesting SSNs, to inform the individual (1) whether disclosure is voluntary or mandatory, (2) by

[1] The Privacy Act defines a system of records as a group of records 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.

what legal authority the SSN is solicited, and (3) what uses will be made of the SSN. The act contains a number of additional provisions that restrict federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or executive order of the president, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under federal programs.

The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii)) – A provision of the Social Security Act bars disclosure by federal, state and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the act also contains criminal penalties for "unauthorized willful disclosures" of SSNs; the Department of Justice would determine whether to prosecute a willful disclosure violation. Because the act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by government entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear if the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to federal, state and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

Appendix III: Federal, State, and County Departments That Reported Maintaining Public Records With SSNs

The following tables provide additional information on the types of departments or agencies that reported maintaining records that are routinely made available to the public and, of those, the ones that reported that their public records contained SSNs.

Table 7: Number of Programs within Federal Agencies That Responded to Our Survey and Maintain Public Records, Identify SSNs on Those Public Records, and Permit Access to Those Records on Their Web Sites

	Maintain public records		Public records identify SSNs		Public has access to records with SSNs via Web site	
	Yes	No	Yes	No	Yes	No
All federal programs	**26**	**31**	**7**	**18**	**3**	**4**
Agriculture	1	3	0	1	0	0
Commerce	0	1	0	0	0	0
Defense	1	2	0	1	0	0
Education	2	3	0	2	0	0
Health Human Services	0	2	0	0	0	0
Housing Urban Development	2	3	0	2	0	0
Interior	2	2	1	1	0	1
Justice	0	5	0	0	0	0
Labor	4	1	0	4	0	0
Transportation	1	3	0	1	0	1
Treasury	3	1	1	2	0	1
Veterans Administration	2	1	1	1	0	1
Small Business Administration	2	2	0	2	0	0
Social Security Administration	3	2	1	1	0	1
Federal Court System	3	0	3	0	3	0

Source: GAO survey of federal agencies.

Table 8: Number and Type of State Departments and Agencies That Maintain Public Records, Identify SSNs on Those Public Records, and Permit Access to Those Records on Their Web Sites

	Maintain public records		Public records identify SSNs		Public has access to records with SSNs via Web site	
	Yes	No	Yes	No	Yes	No
All state departments	**241**	**36**	**75**	**145**	**2**	**70[a]**
State Courts	26	5	19	5	0	17[a]
State Law Enforcement	26	3	8	16	0	8
State Human Services	31	4	8	20	0	8
State Health & Vital Statistics	28	4	7	17	0	7
State Labor	31	6	7	23	1	6
State Licensing	7	0	2	5	0	2
State Education (K-12)	38	4	11	23	1	9
State Education (Higher Education)	14	5	1	12	0	1
State Public Safety	25	5	7	15	0	7
State Corrections	34	4	12	18	0	12

[a]One state entity indicated a "not applicable" response because it did not have a Web site.

Source: GAO survey of state agencies.

Table 9: Number and Type of County Departments and Agencies that Maintain Public Records, Identify SSNs on Those Records, and Permit Access to Those records on Their Web Sites

	Maintain public records		Public records identify SSNs		Public has access to records with SSNs via Web site	
	Yes	No	Yes	No	Yes	No
All county departments	**251**	**46**	**119**	**116**	**11**	**105[a]**
Social Services	35	24	13	19	0	13
Health Department	43	9	10	31	0	10
County Sheriff	55	7	21	28	0	20[a]
Court Clerks	39	3	30	7	2	28
County Recorders	61	2	43	15	9	32
Superintendent of Schools	18	1	2	16	0	2

[a]Two county departments answered "not applicable" because the departments did not have a Web site.

Source: GAO survey of county agencies.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Kay Brown (202) 512-3674
Jacquelyn Stewart (202) 512-7232

Staff Acknowledgments

The following team members contributed to all aspects of this report throughout the review: Lindsay Bach, Jeff Bernstein, Jacqueline Harpp, Daniel Hoy, Raun Lazier, James Rebbe, Vernette Shaw, and Anne Welch. In addition, Richard Burkard, Patrick Dibattista, Joel Grossman, Debra Johnson, Carol Langelier, Minette Richardson, Robert Rivas, Ron Salo, Rich Stana, and William Thompson also made contributions to this report.

GAO's Mission

The General Accounting Office, the 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 daily E-mail alert for newly released products" under the GAO Reports 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