United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Social Security,
Committee on Ways and Means,
House of Representatives

For Release on Delivery
Expected at 2:00 p.m.
Monday, April 29, 2002

SOCIAL SECURITY NUMBERS

SSNs Are Widely Used by Government and Could Be Better Protected

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

GAO-02-691T

Chairman Shaw and Members of the Subcommittee:

Thank you for inviting me here today to discuss government use of Social Security Numbers (SSNs). Although the SSN was originally created in 1936 as a means to track workers' earnings and eligibility for Social Security benefits, today the number is used for myriad non-Social Security purposes in both the private and public sectors. Consequently, the public is concerned with how their personal SSNs are being used and protected. Further, the growth in electronic record keeping and the explosion of the availability of information over the Internet, combined with the rise in reports of identity theft, have heightened this concern.

We have previously reported that SSNs play an important role in public and private sectors' ability to deliver services or conduct business.[1] Today, I will focus on how federal, state, and local governments use SSNs. Specifically, I will discuss (1) the extent and nature of government agencies' use of SSNs as they administer programs to provide benefits and services and the actions government agencies take to safeguard these SSNs from improper disclosure and (2) the extent and nature of governments' use of SSNs when they are contained in public records and the options available to better safeguard SSNs that are traditionally found in these public records.[2] My testimony is based on our ongoing work conducted at your request and that of the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary. To address these issues, we mailed surveys to programs in 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

[1] 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).

[2] We found no commonly accepted definition of public records. For the purposes of this statement, 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.

[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. 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).

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 conducted our work between February 2001 and March 2002 in accordance with generally accepted government auditing standards.

In summary, in delivering services and benefits to the public, federal, state, and county government agencies use SSNs to manage records, verify the eligibility of benefit applicants, collect outstanding debts and conduct research and program evaluation. Using SSNs for these purposes can save the government and taxpayers hundreds of millions of dollars each year. As they make use of SSNs for these purposes, government agencies are taking some steps to safeguard the numbers. However, agencies are not consistently following federal laws regarding the collection of personal information, implementing safeguards to protect SSNs from improper disclosure, or limiting the display of SSN on documents not intended for the public. Moreover, courts at all three levels of government and certain offices at the state and county level maintain records that contain SSNs for the purpose of making them available to the public. Recognizing that these SSNs may be misused by others, some government entities have taken steps to protect the SSNs from public display. For example, some have modified forms so that they can collect SSNs but keep them in a file separate from the public portion of the record. Nonetheless, although public records have traditionally been housed in government offices and court buildings, to improve customer service some government entities are considering placing more public records on the Internet. The ease of access the Internet affords could encourage individuals to engage in information gathering from public records on a broader scale than possible previously. In conclusion, we will be reporting in more detail on these issues at the end of this month and look forward to exploring additional options to better protect SSNs with you as we complete our work.

Background

The use of SSNs by government and the private sector has grown over time, in part because of federal requirements. In addition, the growth in computerized records has further increased reliance on SSNs. This growth in use and availability of the SSN is important because SSNs are often one of the "identifiers" of choice among identity thieves. Although no single federal law regulates the use and disclosure of SSNs by governments, when federal government agencies use them, several federal laws limit the

use and disclosure of the number. [4] Also, state laws may impose restrictions on SSN use and disclosure, and they vary from state to state. 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.

SSN Use Has Grown, in Part Because of Federal Requirements

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 1936, the Social Security Administration (SSA) created a numbering system designed to provide a unique identifier, the SSN, to each individual. The agency uses SSNs to track workers' earnings and eligibility for Social Security benefits, and as of December 1998, SSA had issued 391 million SSNs. Since the creation of the SSN, other entities in both the public and private sectors have begun using SSNs, in part because of federal requirements. 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. (See appendix I for examples of federal laws that authorize or mandate the collection and use of SSNs.) In addition, private businesses, such as financial institutions and health care service providers, also rely on individuals SSNs. In some cases, they require the SSN to comply with federal laws but, at other times, they routinely choose to use the SSNs to conduct business.

In addition, the advent of computerized records further increased reliance on SSNs. 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 of vast amounts of personal information about members of the public, including SSNs, that businesses sell.

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

Identity Thieves Often Use SSNs

The overall 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.[5] 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.

Recent statistics collected by federal and consumer reporting agencies indicate that the incidence of identity theft appears to be growing.[6] 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. 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.[7] Finally, it is difficult to determine how many individuals are prosecuted for identity theft because law enforcement

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

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

[7] 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 office offers fraud alerts that can vary from 2 to 7 years at the discretion of the individual.

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.

Most often, identity thieves use SSNs belonging to real people rather than making one up; however, on the basis of a review of identify 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 themselves 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 the extent to which the government's use of SSNs contributes to this problem as compared to use of SSNs by the private sector.

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 and the Privacy Act. The Freedom of Information Act presumes federal government records are available upon formal request, but exempts certain personal information, such as SSNs. The purpose of the Privacy Act, broadly speaking, is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy by federal agencies. Also, the Social Security Act Amendments of 1990 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

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

SSN use and disclosure for specific programs or activities.[9] 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.

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 computer systems that may contain SSNs.[10] For example, federal agencies must develop an agency-wide information security management program. 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 addition to the SSNs used by program agencies to provide benefits or services, some records that contain SSNs are considered part of the public record and, as such, are routinely made available to the public for review. This is particularly true at the state and county level. Generally, state law governs whether and under what circumstances these records are made available to the public, and they vary from state to state. They 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. Certain records maintained by federal, state, and county courts are also routinely 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. At the federal level, access to

[9] 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.

[10] 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.

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.

SSNs Are Widely Used by Program Agencies at All Levels of Government, but Could Be Better Protected by Them

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. SSNs provide a quick and efficient means of managing records and are used to conduct research and program evaluation. In addition, they are particularly useful when agencies share information with others to verify the eligibility of benefit applicants or to collect outstanding debts. Using SSNs for these purposes can save the government and taxpayers hundreds of millions of dollars each year. As they make this wide use of SSNs, government agencies are taking some steps to safeguard the numbers; however, certain key 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 key information mandated by federal law, such as whether individuals are required to provide their SSNs. Second, although agencies that use SSNs to provide benefits and services are taking steps to safeguard them from improper disclosure, our survey identified potential weaknesses in the security of information systems at all levels of government. Similarly, sometimes government agencies display SSNs on documents not intended for the public, and we found numerous examples of actions taken to limit the presence of SSNs on documents. However, these changes are not systematic and many government agencies continue to display SSNs on a variety of documents.

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

Most of the agencies we surveyed at all levels of government reported using SSNs extensively to administer their programs.[11] As shown in table 1, more agencies reported using SSNs for internal administrative purposes, such as using SSNs 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,

[11] Of the respondents to our survey, 14 state program departments and 13 county program departments reported that they do not obtain, receive, or use the SSN of program participants, service recipients, or individual members of the public. We did not verify this information.

unlike some other personal identifying information, such as names and addresses.

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

Purpose of SSN Use	Federal (N=55)[a]	State (N=244)	County (N=197)
	Percent	Percent	Percent
Internal administrative purposes	82	90	89
Sharing			
Verify applicants' eligibility; monitor accuracy of information individuals provide	73	83	82
Collect debts individuals owe agency/government	40	34	25
Research and Evaluation			
Conduct internal research or program evaluation	53	44	26
Provide data to outside researchers	4	18	7

[a]Total number of possible respondents

Source: GAO surveys of federal, state, and county departments and agencies. Table includes departments and agencies that administer programs and excludes courts, county clerks and recorders, and state licensing agencies. It excludes state departments of motor vehicles and tax administration.

Many agencies also use SSNs to share information with other entities to bolster the integrity of the programs they administer. For example, 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. 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, or employers. As unique identifiers, SSNs help ensure that the agency is matching information on the correct person. Also, some agencies at each level of government reported sharing data containing SSNs to collect debts owed them. Using SSNs for these purposes can save the government and taxpayers hundreds of millions of dollars, such as when SSA matched its data on Supplemental Security Income recipients with state and local correctional facilities to identify prisoners who were no longer eligible for benefits.[12] Doing so helped identify more than $150 million in Supplemental Security Income overpayments and prevented improper payments of more than $170 million over an 8-month period. Finally, SSNs along with other program

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

data, are sometimes used for statistical programs, research, and evaluation, in part because they provide government agencies and others with an effective mechanism for linking data on program participation with data from other sources.[13]

When government agencies that administer programs share records containing individuals' SSNs with other entities, they are most likely to share them with other government agencies.[14] After that, the largest percentage of federal and state program agencies report sharing SSNs with contractors (54 and 39 percent respectively), and a relatively large percentage of county program agencies report sharing with contractors as well (28 percent). Agencies across all levels of government use contractors to help them fulfill their program responsibilities, such as determining eligibility for services and conducting data processing activities. 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.

In addition, all government personnel departments we surveyed reported using their employees' SSNs to fulfill at least some of their responsibilities as employers. Aside from requiring that employers report on their employees' wages to SSA, federal law also requires that states maintain employers' reports of newly hired employees identified by SSN. The national database is used by state child support agencies to locate parents who are delinquent in child support payments. In addition, employers responding to our survey 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.

[13] 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).

[14] 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 programs, 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.

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.[15] Government entities must

- tell individuals whether disclosing their SSNs is mandatory or voluntary;
- 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. 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 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. At the state level, about half of the respondents reported providing individuals with the required information, and at the county level, about 40 percent of the respondents reported doing so.

[15] 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.

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

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. 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.

No uniform guidelines specify what actions governments should take to safeguard personal information that includes SSNs. However, to gain a better understanding of whether agencies had measures in place to safeguard SSNs, we selected eight commonly used practices found in information security programs, and we surveyed the federal, state, and county programs and agencies on their use of these eight practices. 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. In general, when compared to state and county government agencies, a higher percentage of federal agencies reported using most of the eight practices. However, despite the federal government's self-reported more frequent use of these practices relative to the state and counties, it is important to note that since 1996 we have consistently identified significant information security weaknesses across the federal government. We are not aware of a comparable comprehensive assessments of information security for either state or county government. (For additional information on the eight practices we selected and how they fit into the federal framework for an information security program, see appendix II.)

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.[16] Responses to our survey indicate that, when sharing such sensitive information, 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 with these requirements.

Government Agencies Display SSNs on Documents Not Intended for the Public

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. These documents include payroll checks, vouchers for tax credits for childcare, travel orders, and authorization for training outside of the agency. Also, some personnel departments reported displaying employees' SSNs on their employee badges (27 percent of federal respondents, 5 percent of state, and 9 percent of county). Notably, the Department of Defense (DOD), which has over 2.9 million military and civilian personnel, displays SSNs on its military and civilian identification cards. 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 department 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.

In addition to these examples of SSN display, we also 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. For example, the DOD commissary stopped

[16] 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.

requiring SSNs on checks written by members because of concerns about improper use of the SSNs and identity theft.[17] Also, a state comptroller's office changed its procedures so that it now offers vendors the option of not displaying SSNs on their business permits. Finally, some states have passed laws prohibiting the use of SSNs as a student identification number.

These 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.

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

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 licensing agencies and county recorders' offices, have traditionally been repositories for public records that may contain SSNs. In addition, courts at all three levels of government maintain public records that may contain SSNs. Officials who maintain these records told us their responsibility is to preserve the integrity of the record rather than protect the privacy of the individual SSN holder. However, we found examples of some government entities that are trying innovative approaches to protect the SSNs in such records from public display. Moreover, the general public has traditionally gained access to public records by visiting the office that maintains the records, an inconvenience that represents a practical limitation on the volume of SSNs any one person can collect. However, the growth of electronic record-keeping places new pressures on agencies to provide their data to the pubic on the Internet. Although few entities report currently making public records containing SSNs available on the Internet, several officials told us they are considering expanding the volume and type of such records available on their Web site. This would create new opportunities for gathering SSNs on a broader scale. Again, some entities

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

are considering alternatives to making SSNs available on such a wide scale, while others are not.

Many State and County Public Records Contain SSNs

As shown in table 2, more than two-thirds of the courts, county recorders, and state licensing agencies that reported maintaining public records reported that these records contained SSNs.[18] In addition, some program agencies also reported maintaining public records that contain SSNs.

Table 2: 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	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Courts, recorders, and licensing agencies that maintain public records with SSNs	3/3	100	21/31	68	73/95	77
Program agencies that maintain public records with SSNs	4/22	23	54/189	29	46/140	33

Source: Data from GAO survey of federal, state, and county departments and agencies. It excludes state departments of motor vehicles and tax administration.

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 interact with government.[19] 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, which contain SSNs, with their local recorder's office to establish a readily available record of their military service.[20] Also, documents that record financial transactions, such as tax liens and property settlements, contain

[18] Of the respondents to our survey, 20 county recorders and courts and 5 state courts reported that they do not obtain, receive, or use the SSN of program participants, service recipients, or individual members of the public. We did not verify this information.

[19] It differs 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.

[20] 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.

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 non-custodial 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. 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.

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.[21] 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 in documents, such as a petition for an action, a judgment or a divorce decree. 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, such as records pertaining 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.

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 and mandated interest is in preserving 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

[21] 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.

choice but to accept the documents with the SSNs and fulfill the responsibility of their office by making them available to the general public.

Alternatives to Displaying SSNs in Public Records Exist

When creating public documents or records, such as marriage licenses, some government agencies are trying new innovative approaches that protect SSNs from public display. For example, some 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.[22] Changing how the information is captured on the form itself 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 marriage license application so that the form is now in triplicate, and the copy that is available to the general public does not contain the SSN. However, an official told us 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, some courts 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 that is 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 help to reduce the appearance of SSNs. This would include individuals, financial institutions, title companies, and attorneys, who could begin by considering 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.

[22] In some cases, however, the law requires that the SSN appear on the document itself, as on death certificates.

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 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 a particularly lengthy and labor-intensive process to find and redact SSNs. 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.

Traditional Access to Public Records Has Practical Limitations That Would Not Exist if the Records Were Placed 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.[23] Yet, 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 on site where individuals can look up electronic files from a site-specific database. In one of the offices we visited, documents containing SSNs that were otherwise accessible to the public were also made available in bulk to certain groups. When asked about sharing information containing SSNs with other entities, a higher percentage of county recorders reported sharing information containing SSNs with marketing companies,

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

collection agencies, credit bureaus, private investigators, and outside researchers.

Finally, few agencies reported that they place records containing 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. However, 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.

While planning to place more information 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. On the other hand, 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. Given the likely growth of public information on the Internet, the time is right for some kind of forethought about the inherent risk

posed by making SSNs and other personal information available through this venue.

Concluding Observations

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, the gaps in safeguarding SSNs that we have identified create the potential for SSN misuse. Although the extent to which the government's broad use of SSNs contributes to identity theft is not clear, measures to encourage governments to better secure and reduce the display of SSNs could at least help minimize the risk of SSN misuse. It is important to focus on ways to accomplish this. We will be reporting in more detail on these issues at the end of this month and look forward to exploring additional options to better protect SSNs with you as we complete our work.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director, or Kay E. Brown, Assistant Director, Education, Workforce, and Income Security at (202) 512-7215. Individuals making key contributions to this testimony include Lindsay Bach, Jeff Bernstein, Richard Burkard, Jacqueline Harpp, Daniel Hoy, Raun Lazier, Vernette Shaw, Jacquelyn Stewart, and Anne Welch.

Appendix I: 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 HUD programs	Authorizes the secretary of the Department of Housing and Urban Development to require applicants and participants in HUD programs 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

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
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

Appendix II: Our Eight Practices and How They Fit Into the Federal Framework for an Information Security Program

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.[1] The federal framework is consistent with strategies used by private and public organizations that we previously reported have strong information security programs.[2] This 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 to 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.[3] We surveyed the federal, state, and county programs and agencies on their use of these eight practices:

Periodically assess risk

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

[1] 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 Office of Management and Budget guidance.

[2] 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.

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

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)

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