United States Government Accountability 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. EST
Thursday, March 30, 2006

SOCIAL SECURITY NUMBERS

More Could Be Done to Protect SSNs

Statement of Cynthia M. Fagnoni, Managing Director
Education, Workforce, and Income Security Issues

March 30, 2006

SOCIAL SECURITY NUMBERS

More Can Be Done to Protect SSNs

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-586T, a testimony to the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

In 1936, the Social Security Administration established the Social Security number (SSN) to track worker's earnings for Social Security benefit purposes. Since its creation, the SSN has evolved beyond its original purpose and has become the identifier of choice for public and private sector entities. Today, the SSN is a key piece of information often sought by identity thieves. Once the SSN is obtained fraudulently, it can then be used to create false identities for financial misuse or assuming another individual's identity.

Congress and some states have recognized the importance of restricting the use and display of SSNs. GAO has issued a number of reports and testimonies about the various aspects of SSN use in both public and private sectors and what could be done to further protect individual's SSNs. Accordingly, this testimony focuses on describing (1) the use of SSNs by government agencies and certain private sector entities, (2) the federal laws that regulate the use and disclosure of SSNs, and (3) the gaps that remain in protecting the SSN and what more could be done.

www.gao.gov/cgi-bin/getrpt?GAO-06-586T.

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

What GAO Found

SSN use is widespread by both the public and private sectors. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations of their programs. In addition, SSNs are available in a variety of public records. Certain private sector entities routinely obtain SSNs from various public and private sources, and use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. In addition, private sector entities that engage in third party contracting sometimes share SSNs with their contractors for limited purposes.

There is no one law that comprehensively regulates SSN use and protections. However, certain federal laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs. In addition, certain states have begun to enact their own legislation restricting the use and display of SSNs by public and private sector entities, which has subsequently led other states to start enacting similar legislation. Finally, Congress is currently considering several proposals to restrict SSN use and display, similar to state legislation.

Although some action has been taken at the federal and state level to protect SSNs, more could be done. In the course of this work, GAO found that there were gaps in the practices for protecting SSNs within government agencies and across industry sectors, such as a lack of uniformity at all levels of government to assure the security of the SSN; gaps in the federal law and oversight in different industries that share SSNs with their contractors; exposure of SSNs in public records and identification cards under the auspices of the government; and few restrictions on certain entities' abilities to obtain and use SSNs in the course of their business. To address some of these issues, GAO has made recommendations and proposed matters for congressional consideration. To date, OMB has implemented two of these recommendations and some agencies have begun to take steps to eliminate SSNs from their identification cards. Congress is still considering actions to take to address the issues that remain.

Mr. Chairman and Members of the Committees:

I am pleased to be here today to discuss ways to better protect the Social Security Number (SSN). The SSN was created as a means to track workers' earnings and eligibility for Social Security benefits. However, the SSN has evolved beyond its original intended purpose and has become the identifier of choice for public and private sector entities, and is used for numerous non-Social Security purposes. This is significant because SSNs, along with a name and date of birth, are the pieces of information most often sought by identity thieves. Once an SSN is obtained fraudulently, it can then be used to create false identities for financial misuse, assuming another individual's identity, fraudulently obtaining credit, violating immigration laws, or fleeing the criminal justice system. Recent statistics suggest that the incidence of identity theft is rapidly growing. The Federal Trade Commission (FTC) estimated that over a 1-year period nearly 10 million people—or 4.6 percent of the adult U.S. population—discovered that they were victims of some form of identity theft, translating into estimated losses exceeding $50 billion. FTC also reported that most victims of identity theft do not report the crime, and, therefore, the total number of identity theft incidences is unknown.

Over the last few years Congress and some states have recognized the importance of restricting the use and display of SSNs by both public and private sectors. As a result, federal and state laws have begun to be enacted that to some degree protect individual's personal information, including SSNs. GAO has issued a number of reports and testified before this Subcommittee about the various aspects of SSN use in both the public and private sectors. (See related GAO products at the end of this testimony.) Accordingly, you asked us to speak about some of our findings regarding SSN use and protections. My remarks today will focus on (1) the use of SSNs by government agencies and certain private sector entities, (2) the federal laws that regulate the use and disclosure of SSNs, and (3) the gaps that remain in protecting the SSN and what more could be done.

In summary, SSN use is widespread by both the public and private sectors. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations of their programs. In addition, SSNs are available in a variety of public records held by states, local jurisdictions, and courts, appearing in records that document common life events and transactions, such as marriages and home purchases. Certain private sector entities also use SSNs. Information resellers, credit reporting agencies (CRAs), and health care organizations

routinely obtain SSNs from various public and private sources, and use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. In addition, private sector entities that engage in third party contracting sometimes share SSNs with their contractors for limited purposes.

There is no one law that comprehensively regulates SSN use and protections. However, certain federal laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs, but these laws tend to be industry-specific and do not apply broadly. In addition, certain states had begun to enact their own legislation restricting the use and display of SSNs by public and private sector entities, which has subsequently led other states to start enacting similar regulation. Finally, Congress is currently considering several proposals to restrict SSN use and display, similar to state legislation.

Although some action has been taken at the federal and state level to protect SSNs, more could be done. In our prior work, we found gaps in the practices for protecting SSNs by government agencies and across industry sectors. As a result, we made recommendations to federal agencies to address the issues we found and proposed matters for Congress to consider. For example, we found that certain measures that could help protect SSNs are not uniformly in place at all levels of government. In addition, there are gaps in the federal law and oversight in different industries that share SSNs with their contractors, and there are few restrictions placed on certain entities' abilities to obtain and use SSNs in the course of their business. Finally, SSNs are widely exposed in a variety of public records and are still subject to exposure on identity cards issued under federal auspices. To address some of these issues, we made recommendations and proposed matters for congressional consideration. For example, to address gaps in the government uses of SSNs and the exposure of SSNs in public records and on identification cards, we advised Congress to convene a group of government officials to develop a unified approach to safeguarding SSNs. To address the gaps in federal laws that would apply to industries that share SSNs with their contractors, we recommended Congress consider options to restrict the use and display of SSNs to third party contractors.

Background

The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to manage the Social Security program, which resulted in the creation of the SSN.[1] Through a process known as "enumeration," unique numbers are created for every person as a work and retirement benefit record. Today, SSA issues SSNs to most U.S. citizens, but they are also available to non-citizens lawfully admitted to the United States with permission to work. Lawfully admitted noncitizens may also qualify for a SSN for nonwork purposes when a federal, state, or local law requires that they have a SSN to obtain a particular welfare benefit or service. SSA staff collect and verify information from such applicants regarding their age, identity, citizenship, and immigration status.

With the enhancement of computer technologies in recent years, private sector businesses are increasingly computerizing their records; as a result, these enhancements have spawned new businesses activities involving the aggregation of person information. Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information including SSNs for informational services. They may provide their services to a variety of customers, either to specific businesses clients or through the Internet to anyone willing to pay a fee. Consumer reporting agencies, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. CRAs collect information that is considered relevant to a person's credit history, and obtain SSNs from their customers or businesses that furnish data to them, as well as from private and public sources. Organizations that provide health care services also commonly use consumers' SSNs. They obtain SSNs from individuals themselves and companies that offer health care plans.

In recent years, companies have increasingly relied on the use of contractors to perform certain activities and functions related to their business operations. This trend has often been referred to as outsourcing. However, no commonly recognized definition of outsourcing exists, and there has been confusion over whether it encompasses only activities a company performed in-house or includes any activity a company may contract out. According to outsourcing experts, approximately 90 percent of businesses contract out some activity because they find either it is more

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

economical to do so or other companies are better able to perform these activities. Some of the activities companies outsource will require that contractors be provided personal information about the companies' customers in order to perform those activities, in some cases, this information includes SSNs.

Due to the pervasive use of SSNs, individuals are routinely asked to disclose their SSNs, along with other personal identifying information, for numerous purposes. In some instances where individuals provide their SSNs to government entities, documents containing the SSN are routinely made available to the public for inspection. The widespread disclosure of SSNs in public records has raised concern because it can put individuals at increased risk of identity theft. In addition, given the explosion in the Internet use and the ease with which personally identifiable information is accessible, individuals looking to steal someone's identity are increasingly able to do so. According to FTC, it receives roughly 15,000 to 20,000 contacts per week on its hotline and Web site, or through the mail from victims and consumers who want to avoid becoming victims.

Both Government and Private Sector Entities Collect and Use SSNs for a Variety of Purposes

Government entities are generally required by law to collect SSNs to determine individuals' eligibility for services and benefits. SSNs are also widely available in public records maintained by state and local governments and the courts. Certain private sector entities, such as information resellers, CRAs, and healthcare organizations obtain SSNs from public and private sources, or directly from their customers, and use them for various purposes. In addition, banks, securities firms, telecommunication firms, and tax preparers engage in third party contracting and sometimes share SSNs with their contractors for limited purposes.

Government Entities Are Required by Laws and Regulations to Collect SSNs, and Use Them for Various Purposes

As required by a number of federal laws and regulations, agencies at all levels of government frequently collect and use SSNs to administer their programs, to link data for verifying applicants' eligibility for services and benefits, and to conduct program evaluations.[2] For example, the Personal Responsibility and Work Opportunity Act of 1996 mandates that, among other things, states have laws in place to require the collection of SSNs on driver's license applications. Such laws and regulations have contributed to the widespread use of SSNs by government agencies, because the SSN serves as a unique identifier.

Government agencies use SSNs for a variety of purposes. We have found that agencies typically used SSNs to manage their records and to facilitate data sharing to verify an applicant's eligibility for services and benefits.[3] For example, agencies use SSNs

- for internal administrative purposes, which included activities such as identifying, retrieving, and updating records;
- to collect debts owed the government and conduct or support research and evaluations as well as using employees' SSNs for activities such as payroll, wage reporting, and providing employee benefits;
- to ensure program integrity, such as matching records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments; and
- for statistics, research, and evaluation;[4]

[2]GAO, *Social Security: Government and Commercial Use of the Social Security Number Is Widespread*, GAO/HEHS-99-28 (Washington, D.C.: February 16, 1999) and GAO, *Social Security Numbers: Government Benefits from SSN Use, but Could Provide Better Safeguards*, GA0-02-352 (Washington, D.C.: May 31, 2002).

[3]GA0-02-352.

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

SSNs Are Widely Available in Public Records Held by States, Local Jurisdictions, and Courts, but Many of These Agencies Are Taking Steps to Limit Display

SSNs are publicly available throughout the United States, primarily at the state and local levels of government.[5] Based on a survey of federal, state, and local governments, we reported in 2004 that state agencies in 41 states and the District of Columbia were displaying SSNs in public records; this was also true in 75 percent of U.S. counties.[6] We also found that while the number and type of records in which SSNs were displayed varied greatly across states and counties, SSNs were most often found in court and property records.

Public records displaying SSNs are stored in multiple formats that vary by different levels of government. State government offices tended to store such records electronically, while most local government records were stored on microfiche or microfilm. However, our survey found that public access to such records was often limited to inspection of the individual paper copy or request by mail.[7]

We found that few state agencies make public records available on the Internet, although some do so. However, few state or local offices reported any plans to significantly expand Internet access to public records that display SSNs. Based on our survey results, only four state agencies indicated plans to make such records available on the Internet, and one agency planned to remove records displaying SSNs from Internet access.

Private Sector Entities Obtain SSNs from Public and Private Sources and Use Them for Various Purposes

Private sector entities such as information resellers, CRAs, and health care organizations generally obtain SSNs from various public and private sources. Large or well known information resellers have told us they obtain SSNs from various public records, such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate transactions, voter registrations, and professional licenses. They also said

[5]Not all records held by government or public agents are "public" in terms of their availability to any inquiring person. For example, adoption records are generally sealed. Personnel records are often not readily available to the public, although newspapers may publish the salaries of high, elected officials. There is no common definition of public records. However, we define public records as those records generally made available to the public for inspection in their entirety by a federal, state, or local government agency. Such documents are typically accessed in a public reading room, clerk's office, or on the Internet.

[6]GAO, *Social Security Numbers: Governments Could Do More To Reduce Display in Public Records and on Identity Cards*, GAO-05-59 (Washington, D.C.: November 9, 2004).

[7]GAO-05-59.

that they sometimes obtain batch files of electronic copies of jurisdictional public records where available. However, some reseller officials said they are more likely to rely on SSNs obtained directly from their clients, who would voluntarily provide such information for a specific service or product, than those found in public records.[8]

Like information resellers, CRAs also obtain SSNs from public and private sources. CRA officials have told us that they obtained SSNs from public sources, such as bankruptcy records. We also found that these companies obtained SSNs from other information resellers, especially those that specialized in obtaining information from public records. However, CRAs are more likely to obtain SSNs from businesses that subscribe to their services, such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies. Therefore, individuals who provide these businesses with their SSNs for reasons such as applying for credit would subsequently have their charges and payment transactions, accompanied by the SSN, reported to the CRAs.

Health care organizations, including health care insurance plans and providers, are less likely to obtain SSN data from public sources. Health care organizations typically obtained SSNs either from individuals themselves or from companies that offer health care plans. For example, subscribers or policyholders enrolled in a health care plan provide their SSN as part of their health care plan application to their company or employer group. In addition to health care plans, health care organizations also included health care providers, such as hospitals. Such entities often collected SSNs as part of the process of obtaining information on insured people. However, health care provider officials told us that, particularly with hospitals, the medical record number is the primary identifier, rather than the SSN.

We found that the primary use of the SSN by information resellers, CRAs, and health care organizations alike was to help verify the identity of an individual. Large information resellers said they generally use the SSN as

[8]GAO, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, GAO-04-11 (Washington, D.C.: January 22, 2004).

an identity verification tool. They also use it for internal matching purposes of its databases, as a factor in identifying individuals for their product reports, or for conducting investigations for their clients for resident screening or employment screening. CRAs use SSNs as the primary identifier of individuals that enables them to match the information they receive from their business clients with information stored in their databases on individuals. Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN is the primary factor that ensures that incoming data is matched correctly with an individual's information on file. We found that in some cases CRAs and information resellers can sometimes be the same entity, a fact that blurs the distinction between the two types of businesses but does not affect the use of SSNs by these entities. Finally, health care organizations also use the SSN to help verify the identity of individuals. These organizations use SSNs, along with other information such as name, address, and date of birth, as a factor in determining a member's identity.

Private sector companies also share customers' SSNs with their contractors. Banks, investment firms, telecommunication companies, and tax preparation companies we interviewed routinely obtain SSNs from their customers for authentication and identification purposes.[9] All these companies contracted out various services, such as data processing, administrative, and customer service functions. Although these companies may share consumer information, such as SSNs, with contractors that provide services to their customers, company officials said that they only share such information with their contractors for limited purposes, generally when it is necessary or unavoidable.

The companies we contacted provided us with standard contract forms they use in contracting with service providers to safeguard customers' personal information, such as SSNs, from misuse.[10] In general, the types of provisions these companies included in their standard contract forms included electronic and physical data protections, audit rights, data breach notifications, subcontractor restrictions, and data handling and disposal requirements. We found that most of the companies we interviewed had established some type of due diligence or credentialing process to verify

[9]*GAO, Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs*, GAO-06-238 (Washington, D.C.: January 23, 2006).

[10]GAO-06-238.

the reliability of potential contractors prior to and during contract negotiations. Furthermore, we found that some industry associations have voluntarily developed guidance for their members regarding the sharing of personal information with third parties.

No Single Law Governs the Use and Disclosure of SSNs Although Various Laws Have Been Enacted That Help Protect SSNs

Although no single law comprehensively governs the use and disclosure of SSNs, certain federal laws restrict the use and disclosure of personal information, including SSNs, by government agencies or private sector entities. These laws, however, tend to be directed at specific industries or governmental agencies and often do not apply broadly across public and private sectors or across private sector industries. For example, the overall use and disclosure of SSNs by the federal government is restricted under the Privacy Act, which, broadly speaking, seeks 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. The Privacy Act requires that any federal, state, or local government agency, when requesting an SSN from an individual, tell individuals whether disclosing their SSN is mandatory or voluntary, cite the statutory or other authority under which the request is being made, and state what uses it will make of the individual's SSN.

Other federal laws have also placed restrictions on private sector entities' use and disclosure of consumers' personal information, including SSNs. These include the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transaction Act (FACTA), the Gramm-Leach-Bliley Act (GLBA), the Drivers Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA). As shown in table 1, some of these federal laws either restrict certain private sector entities from disclosing personally identifiable information to specific purposes or with whom the information is shared. In addition, certain industries, such as the financial services industry, are required to protect individuals' personal information to a greater degree than entities in other industries.

Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information

Federal Laws	Restrictions
Fair Credit Reporting Act	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Fair and Accurate Credit Transactions Act	Amends FCRA to allow, among others things, consumers who request a copy of their credit report to also request that the first 5 digits of their SSN (or similar identification number) not be included in the file; requires consumer reporting agencies and any business that use a consumer report to adopt procedures for proper disposal.
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to nonaffiliated third parties.
Health Insurance Portability and Accountability Act	Protects the privacy of health information that identifies an individual and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis

Congress has also introduced a federal statute that criminalizes fraud in connection with the unlawful theft and misuse of personal identifiable information. In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act (Identity Theft Act). The act made it a criminal offense for a person to "knowingly transfer, possess, or use without lawful authority," another person's means of identification "with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law." Under the act, a name or Social Security number is considered a "means of identification" and a number of cases have been prosecuted under this law.

Many states have begun to enact laws to restrict the use and display of SSNs. (See appendix 1 for a listing of state laws previously reported by GAO.) After one state took action, other states followed in enacting similar laws. For example, in 2001, California enacted a law restricting the use and display of SSNs, which generally prohibited companies and persons from engaging in certain activities, such as posting or publicly displaying SSNs, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted. In addition, California enacted a law containing notification requirements in the event of a security breach where a business or a California state agency is required to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Subsequently, other states have enacted laws restricting the use and display of SSNs. Specifically, in our prior work, we identified 13 others states—Arizona, Arkansas, Connecticut, Georgia, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas, Utah, and Virginia—that have each passed laws similar to California's.[11] While some states, such as Arizona, have enacted virtually identical SSN use and display restrictions, other states have modified the restrictions in various ways. For example, unlike the California law, which prohibits the use of the full SSN, the Michigan statute prohibits the use of more than four sequential digits of the SSN. The Michigan law also contains a prohibition against the use of SSNs on identification and membership cards, permits, and licenses. Missouri's law includes a prohibition against requiring an individual to use his or her SSN as an employee number. Oklahoma's law is unique in that it only limits the ways in which employers may use their employees' SSNs, and does not apply more generally to other types of transactions and activities.

Some states have recently enacted other types of restrictions on the uses of SSNs as well. Arkansas, Colorado, and Wisconsin limit the use of a student's SSN as a student identification number.[12] New Mexico requires businesses that have acquired consumer SSNs to adopt internal policies to limit access to authorized employees.[13] Texas recently enacted a law requiring businesses to properly dispose of business records that contain a customer's personal identifying information, which is defined to include SSNs.[14]

Other recent state legislation includes new restrictions on state and local government agencies. For example, South Dakota law prohibits the display of SSNs on all driver's licenses and nondriver's identification

[11] See Arkansas (Ark. Code Ann. § 4-86-107 (2005)); Arizona (Ariz. Rev. Stat. § 44-1373 (2004)); Connecticut (Conn. Gen. Stat. § 42-470 (2003)); Georgia (Ga. Code Ann. § 33-24-57.1 (2003)); Illinois (815 Ill. Comp. Stat. 505/2QQ (2004)); Maryland (Md. Code Ann., Com. Law § 14-3301 et seq. (2005)); Michigan (Mich. Comp. Laws § 445.81 et seq. (2004)); Minnesota (Minn. Stat. § 325E.59 (2005)); Missouri (Mo. Rev. Stat. § 407.1355 (2003)); Oklahoma (Okla. Stat. tit. 40, § 173.1 (2004)); Texas (Tex. Bus. & Com. Code Ann. 35.58 (2003)); Utah (Utah Code Ann. § 31A-21-110 (2004)); and Virginia (Va. Code Ann. § 59.1-443.2 (2005)).

[12] Ark. Code Ann. § 6-18-208 (2005); Colo. Rev. Stat. § 23-5-127 (2003); and Wis. Stat. § 36.32 (2001).

[13] N.M. Stat. Ann. § 57-12B-1 et seq. (2003).

[14] Tex. Bus. & Com. Code Ann. § 35.48 (2005).

cards,[15] while Indiana law generally prohibits a state agency from releasing a SSN unless otherwise required by law.[16] In addition, as of January 1, 2007, a Nevada law will require governmental agencies, except in certain circumstances, to ensure that the SSNs recorded in their books and on their records are maintained in a confidential manner.[17]

We also identified four states that have passed legislation containing notification requirements in the event of a security breach. For example, New York recently enacted a law requiring such notifications.[18] California requires a business or a California state agency to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[19] In the last year, this law forced several large companies to notify individuals that their information was compromised because of certain circumstances. Under a Nevada law, government agencies and certain persons who do business in the state must notify individuals if their personal information is reasonably believed to have been compromised.[20] Similarly, Georgia requires certain private sector entities to notify their customers if a security breach occurred that compromised their customers' personal information, such as their SSNs.[21]

In addition, we found that some state offices were beginning to take measures to change the way in which they displayed or shared SSNs in public records. For example, we found that many state agencies had restricted access to or redacted—covered or otherwise hidden from view—SSNs from public versions of records. Specific restrictions and other actions state agencies reported taking included blocking or removing SSNs from electronic versions of records, allowing individuals identified in the record to request removing their SSN from the publicly available version, replacing SSNs with alternative identifiers, and restricting access only to individuals identified in the records.

[15]S.D. Codified Laws § 32-12-17.13 (2005).

[16]Ind. Code § 4-1-10-1 et seq. (2005).

[17]Nev. Rev. Stat.§ 239.030 (2005).

[18]N.Y. State Tech. Law §208 (2005).

[19]Cal. Civ. Code § 1798.29 (2002); 1798.82 (2002).

[20]Nev. Rev. Stat. §603A.220 (2005).

[21]Ga. Code Ann. § 10-1-910 et seq. (2005).

Finally, Congress is currently considering consumer privacy legislation, which in some cases includes SSN restrictions. In 2005, there were more than 20 proposed bills pending before the U.S. House and Senate.[22] In some cases, the provisions being considered mirrored provisions in enacted state laws. For example, some proposed legislation included prohibitions on the display of SSNs, similar to a Colorado law, while other proposed legislation address the solicitation of SSNs by public and private sector entities. In addition, some federal privacy legislation also proposed consumer safeguards, such as security freezes and prohibitions on the sale and purchase of SSNs.

More Could Be Done To Protect SSNs

Although laws at both state and federal levels have helped to restrict SSN display and protect individual's personal information, clearly gaps remain. We have issued a number of reports for this Subcommittee that have looked at the collection, use, and protections of SSNs by federal agencies and private sector entities. In some cases where federal action could be taken, we have proposed matters for congressional consideration to explore legislative actions or recommendations to a federal agency to address problems we found. In other cases, mainly those that relate to private sector entities, we have proposed a matter for Congressional consideration. OMB has implemented two of our recommendations and Congress is still considering what actions need to be taken.

Prior Work Found Gaps in the Protections of SSNs

In our review of government uses of SSNs, we reported that certain measures that could provide more assurances that SSNs obtained by government entities are secure are not universally in place at any level of government.[23] Agencies that deliver services and benefits use SSNs to administer programs and took some steps to safeguard SSNs. However, when federal, state, and county agencies request SSNs, they did not consistently inform 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 took action to limit the display of SSNs on documents that were not intended to be public but may be viewed by others, these actions sometimes took place in a piecemeal manner rather than as a result of a systematic effort.

[22]GAO, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain*, GAO-05-1016T (Washington, D.C.: September15, 2005)

[23]GAO-02-352

In our reviews of private sector entities' collection and use of SSNs, we found gaps in how different industries are covered by federal laws protecting individual's personal information. In our third party contractors' review, we reported that federal regulation and oversight of SSN sharing varies across four industries we reviewed, revealing gaps in federal law and agency oversight for different industries that share SSNs with their contractors.[24] For example, federal law and oversight of the sharing of personal information in the financial services industry is very extensive: financial services companies must comply with GLBA requirements for safeguarding customer's personal information, and regulators have an examination process in place that includes determining whether banks and securities firms are safeguarding this information. IRS has regulations and guidance in place to restrict the disclosure of SSNs by tax preparers and their contractors, but does not perform periodic reviews of tax preparers' compliance. FCC does not have regulations covering SSNs and also does not periodically review telecommunications companies to determine whether they are safeguarding such information. Companies in the industries we reviewed relied on accepted industry practices and primarily used the terms of their contracts to safeguard personal information, including SSNs they shared with outside contractors.

We also found that there are few restrictions placed on certain entities' abilities such as information resellers to resell SSNs in the course of their business. Although certain federal laws have some restrictions on reselling nonpublic personal information, these laws only apply to certain types of private sector entities, such as financial institutions.

In our review of SSNs in public records, we found that SSNs are widely exposed to view in a variety of public records and are still subject to exposure on identity cards issued under federal auspices.[25] The number and type of records in which SSNs are displayed varies greatly for both states and counties, and SSNs are available in some federal court records. A number of government agencies and oversight bodies are taking steps to eliminate the open display of SSNs. For example, some actions state agencies reported taking included blocking or removing SSNs from electronic versions of records, and replacing SSNs with alternative identifiers. However, such initiatives to protect the SSN may slow its

[24]GAO-06-238.

[25]GAO-05-59.

misuse, but the absence of uniform and comprehensive policy is likely to leave many individuals vulnerable.

Finally, although they are not displayed in public records en masse, we found that millions of SSNs are still subject to exposure on individual identity cards issued under federal auspices. We found that in 2004 an estimated 42 million Medicare cards displayed entire 9-digit SSNs, as did approximately 8 million Department of Defense (DOD) insurance cards and 7 million Department of Veterans Affairs (VA) beneficiary cards. Some of these agencies have begun taking action to remove SSNs from identification cards. For example, VA is eliminating SSNs from 7 million VA identification cards and is replacing cards with SSNs or issuing new cards without SSNs from 2004 through 2009, until all such cards have been replaced. DOD has begun replacing approximately 6 million health insurance cards that display SSNs with cards that do not display the bearer's SSN, but continues to include SSNs on approximately 8 million military identification cards. The Centers for Medicare and Medicaid Services, with the largest number of cards displaying the entire 9-digit SSN, does not plan to remove the SSN from Medicare identification cards.

GAO Has Proposed Matters for Congressional Consideration and Recommendations

In order to address the issues we found, GAO has proposed matters for congressional consideration and recommended that a federal agency take action. To date, OMB has implemented two of our three recommendations, but Congress is still considering what other actions to take.

- In order to address the problems we found with how government entities assure the security of SSNs, we proposed that Congress consider convening a representative group of federal, state, and local officials to develop a unified approach to safeguarding SSNs used in all levels of government. 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. However, these requirements may not be uniformly observed. We presented a matter for congressional consideration to facilitate intergovernmental collaboration in strengthening safeguards at the state and local levels. We also made two recommendations to the Office of Management and Budget that it direct federal agencies to review their practices for securing SSNs and providing required information, and advise all federal, state, and local governments of the applicability of the Privacy Act to their uses of SSNs. OMB has implemented both our recommendations.

- In our report on third party contactors' uses of SSNs, we recommended that Congress consider possible options for addressing the gaps in existing federal requirements for safeguarding SSNs shared with contractors. The current gaps do not provide incentives for companies to commit to protecting personal information. Each industry is subject to different federal oversight and is often left to decide what established practices for safeguarding SSNs and other consumer information it wishes to follow. We suggested that one approach Congress could take would be to require industry-specific protections for the sharing of SSNs with contractors where such measures are not already in place. For example, Congress could consider whether the Telecommunications Act of 1996 should be amended to address how that industry shares SSNs with contractors. Alternatively, we suggested that Congress could take a broader approach. For example, in considering proposed legislation that would generally restrict the use and display of SSNs, Congress could also include a provision that would explicitly apply this restriction to third party contractors. We stated that with either approach, Congress would want to establish a mechanism overseeing compliance by contractors and enforcement.

- In our report on the display of SSNs on identification cards and in public records, we recommended that OMB identify all those federal activities that require or engage in the display of 9-digit SSNs on health insurance, identification, or any other cards issued to federal government personnel or program beneficiaries, and devise a governmentwide policy to ensure a consistent approach to this type of display. Although SSA has authority to issue policies and procedures over the Social Security cards that it issues, it does not have authority over how other federal agencies use and display SSNs. Rather, it is up to individual government agencies to have their own policies for the cards issued under their authority. The lack of a broad, uniform policy allows for inconsistent, but persistent exposure of the SSN. OMB has not yet taken action on our recommendation but said at the time we issued our report they would consider it. With regard to SSN exposure in public records, we again noted that it would be constructive for a representative group of federal, state, and local officials to develop a unified approach to safeguarding SSNs used in all levels of government, particularly those displayed in public records.

- Finally, with regard to private sector entities, such as information resellers reselling personal information, including SSNs, we noted that there are few restrictions placed on these entities ability to obtain, use, and resell SSNs for their businesses. The federal laws that have some restrictions can be interpreted broadly. The broad interpretation

combined with the uncertainty about the application of the exceptions suggest that reselling personal information—including SSNs—is likely to continue.

Conclusions

The use of SSNs by both public and private sector entities is likely to continue given that it is used as the key identifier by most of these entities and there is currently no other widely accepted alternative. Given the significance of the SSN in committing fraud or stealing a person's identity, it is imperative that steps be taken to protect it. Without proper safeguards in place, SSNs will remain vulnerable to misuse, thus adding to the growing number of identity theft victims.

SSNs are still widely used and publicly available, although becoming less so. State legislatures have begun to place restrictions on SSNs by enacting laws that restrict the use and display of SSNs and prohibit the theft of individuals' personal information. Yet, more could be done to protect SSNs. As Congress continues to propose and consider legislation to protect individuals' personal information, gaps in protections that have already been identified could help focus the debate on the areas that could be addressed immediately based on our work in order to prevent SSNs and other personal information from being misused.

At this Subcommittee's request, we are continuing work on SSNs and the ease with which they can be purchased from Internet information resellers. We look forward to supporting continued congressional consideration of these important policy issues. That concludes my testimony, and I would be pleased to respond to any questions the subcommittee has.

GAO Contacts and Staff Acknowledgments

For further information regarding this testimony, please contact Cindy M. Fagnoni, Managing Director; or Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues at (202) 512-7215. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony, include Tamara Cross, Joel Marus and Sheila McCoy.

Appendix I: Selected State SSN Laws Previously Reported by GAO

Type of Law	Enacting States
Imposes Limits on State and Local Governments, including Restrictions on Public Disclosure	Connecticut Delaware Florida Georgia Hawaii Indiana Minnesota Nebraska Nevada New Jersey North Dakota Oregon South Carolina Tennessee Texas Virginia West Virginia
Limits Use and Display of SSNs	Arizona Arkansas California Connecticut Georgia Illinois Maryland Michigan Minnesota Missouri Oklahoma Texas Utah Virginia
Limits Use of SSNs on Drivers' Licenses	Indiana North Dakota South Dakota West Virginia

Type of Law	Enacting States
Requires Notification of Security Breaches	California Georgia Nevada New York
Prohibits Certain Activities Related to Identity Theft	Arizona Idaho New York
Limits or Prohibits Use of SSN as Student ID Number	Arkansas Colorado Wisconsin
Authorizes Redaction of SSNs in Certain Public Records	California New Jersey
Limits Certain Activities of Financial Institutions	North Dakota Vermont
Prohibits Businesses From Requiring SSNs as a Condition of Doing Business	New Mexico Rhode Island
Requires Development of Employee Access Policies	New Mexico
Requires Business to Properly Dispose of Business Records Containing Customers' Personal Information	Texas
Provides Identity Theft Victim Assistance	Washington
Requires that SSNs be Truncated for Certain Public Records	Louisiana
Requires Third Party Contracting Protections	California

Source: GAO Analysis

Related GAO Products

Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs. GAO-06-238. Washington, D.C.: January 23, 2006.

Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain. GAO-05-1016T. Washington, D.C.: September 15, 2005.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary in Private and Public Sectors. GAO-04-1099T. Washington, D.C.: September 28, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary. GAO-04-768T. Washington, D.C.: June 15, 2004.

Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information. GAO-04-11. Washington, D.C.: January 22, 2004.

Social Security Numbers: Ensuring the Integrity of the SSN. GAO-03-941T. Washington, D.C.: July 10, 2003.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.:May 31, 2002.

Social Security: Government and Commercial Use of the Social Security Number is Widespread. GAO/HEHS-99-28. Washington, D.C.: February 16, 1999.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548