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 10:00 a.m. EDT
Thursday, June 21, 2007

SOCIAL SECURITY NUMBERS

Use is Widespread and Protection Could Be Improved

Statement of Daniel Bertoni, Director
Education, Workforce, and Income Security Issues

GAO-07-1023T

June 21, 2007

SOCIAL SECURITY NUMBERS

Use is Widespread and Protection Could be Improved

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-1023T, a testimony before the Committee On Ways and Means, Subcommittee on Social Security

Why GAO Did This Study

Since its creation, the Social Security number (SSN) has evolved beyond its intended purpose to become the identifier of choice for public and private sector entities, and it is now used for myriad non-Social Security purposes. This is significant because a person's SSN, along with name and date of birth, are the key pieces of personal information used to perpetrate identity theft. Consequently, the potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs. Accordingly, this testimony focuses on describing the (1) use of SSNs by government agencies, (2) use of SSNs by the private sector, and (3) vulnerabilities that remain to protecting SSNs.

For this testimony, we primarily relied on information from our prior reports and testimonies that address public and private sector use and protection of SSNs. These products were issued between 2002 and 2006 and are listed in the Related GAO Products section at the end of this statement. We conducted our reviews in accordance with generally accepted government auditing standards.

What GAO Found

A number of federal laws and regulations require agencies at all levels of government to frequently collect and use SSNs for various purposes. For example, agencies frequently collect and use SSNs to administer their programs, link data for verifying applicants' eligibility for services and benefits, and conduct program evaluations.

In the private sector, certain entities, such as information resellers, collect SSNs from public sources, private sources, and their customers and use this information for identity verification purposes. In addition, banks, securities firms, telecommunication firms, and tax preparers engage in third party contracting, and consequently sometimes share SSNs with their contractors for limited purposes.

Vulnerabilities persist in federal laws addressing SSN collection and use by private sector entities. In particular, we found variation in how different industries are covered by federal laws protecting individuals' personal information. For example, although federal laws place restrictions on reselling some personal information, these laws apply only to certain types of private sector entities, such as financial institutions. Consequently, information resellers are not covered by these laws, and there are few restrictions placed on these entities' ability to obtain, use, and resell SSNs for their businesses. Vulnerabilities also exist in federal law and agency oversight for different industries that share SSNs with their contractors. For example, while federal law and oversight of the sharing of personal information in the financial services industry are very extensive, federal law and oversight of the sharing of personal information in the tax preparation and telecommunications industries are somewhat lacking. Moreover, in our Internet resellers report, several resellers provided us with truncated SSNs showing the first five digits, though other information resellers and consumer reporting agencies truncate SSNs to show the last four digits. Therefore, because of the lack of SSN truncation standards, even truncated SSNs remain vulnerable to potential misuse by identity thieves and others. While we suggested that the Congress consider enacting standards for truncating SSNs or delegating authority to the Social Security Administration or some other governmental entity to do so, SSN truncation standards have yet to be addressed at the federal level.

www.gao.gov/cgi-bin/getrpt?GAO-07-1023T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Daniel Bertoni at (202) 512-7215, bertonid@gao.gov.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss ways to better protect the Social Security number (SSN), which was originally created as a means to track workers' earnings and eligibility for Social Security benefits. Since its creation, the SSN has evolved beyond its intended purpose to become the identifier of choice for public and private sector entities and is now used for myriad non-Social Security purposes. This is significant because a person's SSN, along with name and date of birth, are the key pieces of personal information used to perpetrate identity theft. Consequently, the potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs.

Over the last several years, the Congress and some states have recognized the importance of restricting the use and display of SSNs by both the public and private sectors. As a result, federal and state laws have been enacted that to some degree protect individuals' personal information, including SSNs. However, the continued use of and reliance on SSNs by public and private sector entities, as well as the potential for their misuse, underscore the importance of identifying areas that can be further strengthened. 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. Accordingly, my remarks today will focus on describing the (1) use of SSNs by government agencies, (2) use of SSNs by the private sector, and (3) vulnerabilities that remain to protecting SSNs.

In summary, a number of federal laws and regulations require agencies at all levels of government to frequently collect and use SSNs for various purposes. For example, agencies frequently collect and use SSNs to administer their programs, link data for verifying applicants' eligibility for services and benefits, and conduct program evaluations. In the private sector, certain entities, such as information resellers, collect SSNs from public sources, private sources, and their customers and use this information for identity verification purposes. In addition, banks, securities firms, telecommunication firms, and tax preparers sometimes share SSNs with their contractors for limited purposes. Although laws at both the federal and state levels have helped to restrict SSN use and display, and both public and private sector entities have taken some steps to further protect this information, several vulnerabilities remain. For example, federal laws addressing SSN use and collection in the private sector continue to leave SSNs maintained by certain industries vulnerable to misuse by identity thieves and others.

For this testimony, we primarily relied on information from our prior reports and testimonies that address public and private sector use and protection of SSNs. These products were issued between 2002 and 2006 and are listed in the Related GAO Products section at the end of this statement. We conducted our reviews in accordance with generally accepted government auditing standards.

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, as well as non-citizens lawfully admitted to the United States with permission to work. Because the SSN is unique for every individual, both the public and private sectors increasingly use it as a universal identifier. This increased use, as well as increased electronic record keeping by both sectors, has eased access to SSNs and potentially made this information more vulnerable to misuse, including identity theft.

Specifically, SSNs are a key piece of information used to create false identities for financial misuse or to assume another individual's identity. Most often, identity thieves use SSNs belonging to real people. However, the Federal Trade Commission's (FTC) identity theft victim complaint data has shown that only 30 percent of identity theft victims know how thieves obtained their personal information. The FTC estimated that over a 1-year period, nearly 10 million people discovered they were victims of identity theft, translating into estimated losses of billions of dollars.

Federal Laws Affecting SSN Use and Disclosure

There is no one law that regulates the overall use of SSNs by all levels and branches of government. However, the use and disclosure of SSNs by the federal government is generally restricted under the Privacy Act of 1974. Broadly speaking, this act 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. Section 7 of the act requires that any federal, state, or local government agency, when requesting an SSN from an individual, tell individuals whether disclosing

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

the 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.

Additional federal laws also place restrictions on public and private sector entities' use and disclosure of consumers' personal information, including SSNs, in specific instances. As shown in table 1, some of these laws require certain industries, such as the financial services industry, to protect individuals' personal information to a greater degree than entities in other industries.

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

Federal laws	Restrictions
Fair Credit Reporting Act (FCRA)	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Fair and Accurate Credit Transactions Act (FACTA)	Amends FCRA to allow, among others things, consumers who request a copy of their credit report to also request that the first five 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 (GLBA)	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to nonaffiliated third parties.
Drivers Privacy Protection Act (DPPA)	Prohibits obtaining and disclosing SSNs and other personal information from a motor vehicle record except as expressly permitted under the law.
Health Insurance Portability and Accountability Act (HIPAA)	Protects the privacy of health information that identifies an individual (including by SSNs) and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis.

In 1998, Congress also enacted a federal statute that criminalizes fraud in connection with the unlawful theft and misuse of personal identifiable information, including SSNs. The Identity Theft and Assumption Deterrence 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, an individual's name or Social Security number is considered a "means of identification." In addition, in 2004, the Identity Theft Penalty Enhancement Act established the offense of aggravated identity theft in the federal criminal court, which is punishable by a mandatory two-year prison term.

State Laws Affecting SSN Use and Disclosure

Many states have also enacted laws to restrict the use and display of SSNs.[2] For example, in 2001, California enacted a law that generally prohibited companies and persons from engaging in certain activities with SSNs, 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 our prior work, we identified 13 states—Arizona, Arkansas, Connecticut, Georgia, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas, Utah, and Virginia—that have passed laws similar to California's. [3] While some states, such as Arizona, have enacted virtually identical restrictions on the use and display of SSNs, 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.

Some states have also enacted other types of restrictions on the uses of SSNs. For example, Arkansas, Colorado, and Wisconsin prohibit the use of a student's SSN as an identification number. [4] Other recent state legislation places restrictions on state and local government agencies, such as Indiana's law that generally prohibits state agencies from releasing SSNs unless otherwise required by law. [5]

[2] For more information on state laws relating to SSN use and disclosure, see GAO, *Social Security Numbers: More Could Be Done to Protect SSNs*, GAO-06-586T (Washington, D.C.: March 30, 2006) GAO, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain*, GAO-05-1016T (Washington, D.C.: Sept.15, 2005).

[3] 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)).

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

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

Government Agencies Collect and Use SSNs for a Variety of Purposes

A number of federal laws and regulations require agencies at all levels of government to frequently collect and use SSNs for various purposes. Beginning with a 1943 Executive Order issued by President Franklin D. Roosevelt, all federal agencies were required to use the SSN exclusively for identification systems of individuals, rather than set up a new identification system. In later years, the number of federal agencies and others relying on the SSN as a primary identifier escalated dramatically, in part, because a number of federal laws were passed that authorized or required its use for specific activities. For example, agencies use SSNs

- for internal administrative purposes, which include activities such as identifying, retrieving, and updating records;
- to collect debts owed to the government and conduct or support research and evaluations, as well as use 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.[6]

Table 2 provides an overview of federal statutes that address government collection and use of SSNs. In some cases, these statutes require that state and local government entities collect SSNs.

[6]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.

Table 2: Examples of Federal Statutes that Authorize or Mandate the Collection or Use of SSNs

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

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

Souce: GAO review of applicable federal laws.

Some government agencies also collect SSNs because of their responsibility for maintaining public records, which are those records generally made available to the public for inspection by the government. Because these records are open to the public, such government agencies, primarily at the state and local levels, provide access to the SSNs sometimes contained in those records.[7] 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 displayed SSNs in public records; this was also true in 75 percent of U.S. counties.[8] 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, such as electronic, microfiche and microfilm, or paper copy. While our prior work found that public access to such records was often limited to inspection of the individual paper copy in public reading rooms or clerks' offices, or request by mail, some agencies also made public records available on the Internet.

In recent years, some agencies have begun to take measures to change the ways in which they display or provide access to SSNs in public records. For example, some state agencies have reported removing SSNs from electronic versions of records, replacing SSNs with alternative identifiers in records, restricting record access to individuals identified in the records, or allowing such individuals to request the removal of their SSNs from these records.

[7]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.

[8]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).

Private Sector Entities Collect SSNs from Various Sources for Identity Verification Purposes

Certain private sector entities, such as information resellers, consumer reporting agencies (CRAs), and healthcare organizations collect SSNs from public and private sources, as well as their customers, and primarily use SSNs for identity verification 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, generally when it is necessary and unavoidable.

Private Sector Entities Collect SSNs from Both Public and Private Sources

Information resellers are businesses that specialize in amassing personal information, including SSNs, and offering informational services. They provide their services to a variety of customers, such as specific businesses clients or through the Internet to the general public. Large or well known information resellers reported that they obtain SSNs from various public records, such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, and real estate transactions. [9] However, some of these resellers said they are more likely to rely on SSNs obtained directly from their clients, who may voluntarily provide such information, than those found in public records. In addition, in our prior review of information resellers that offer their services through the Internet, we found that their Web sites most frequently identified public or nonpublic sources, or both, as their sources of information.[10] For example, a few Internet resellers offered to conduct background investigations on individuals by compiling information from court records and using a credit bureau to obtain consumer credit data.

CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Like information resellers, CRAs also obtain SSNs from public and private sources. For example, CRA officials reported that they obtain SSNs from public sources, such as bankruptcy records.[11] We also found that these companies obtain SSNs from other information resellers, especially those that specialize in collecting information from public records. However, CRAs

[9] 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).

[10] GAO, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs*, GAO-06-495 (Washington, D.C.: May 17, 2006).

[11] GAO-04-11.

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.

Organizations that provide health care services, including health care insurance plans and providers, are less likely to obtain SSNs from public sources. These organizations typically obtain SSNs either from individuals themselves or from companies that offer health care plans. For example, individuals enrolling in a health care plan provide their SSNs as part of their plan applications. In addition, health care providers, such as hospitals, often collect SSNs as part of the process of obtaining information on insured people.

Private Sector Entities Primarily Use SSNs to Verify Individuals' Identities

We found that the primary use of SSNs by information resellers, CRAs, and health care organizations is to help verify the identity of individuals. Large information resellers reported that they generally use the SSN as an identity verification tool, though they also use it for matching internal databases, identifying individuals for their product reports, or conducting resident or employment screening investigations for their clients. CRAs use SSNs as the primary identifier of individuals in order to match information they receive from their business clients with information on individuals already stored in their databases. Finally, health care organizations also use the SSN, together with information such as name, address, and date of birth, for identity verification.

In addition to their own direct use of customers' SSNs, private sector entities also share this information with their contractors. According to experts, approximately 90 percent of businesses contract out some activity because they find either it is more economical to do so or other companies are better able to perform these activities. Banks, investment firms, telecommunication companies, and tax preparation companies we interviewed for our prior work routinely obtain SSNs from their customers for authentication and identification purposes and contract with other companies for various services, such as data processing, administrative, and customer service functions. [12] Company officials reported that customer information, such as SSNs, is shared with contractors for limited

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

purposes, generally when it is necessary or unavoidable. Further, these companies included certain provisions in their standard contact forms aimed at safeguarding customer's personal information. For example, forms included electronic and physical data protections, audit rights, data breach notifications, subcontractor restrictions, and data handling and disposal requirements.

Vulnerabilities Remain to Protecting SSNs in both the Public and Private Sectors

Although federal and state laws have helped to restrict SSN use and display, and public and private sector entities have taken some steps to further protect this information, our prior work identified several remaining vulnerabilities. While government agencies have since taken actions to address some of the identified SSN protection vulnerabilities in the public sector, private sector vulnerabilities that we previously identified have not yet been addressed. Consequently, in both sectors, vulnerabilities remain to protecting SSNs from potential misuse by identity thieves and others.

Government Agencies Have Taken Additional Actions to Address SSN Protection, yet Vulnerabilities Remain

In our prior work, we found that several vulnerabilities remain to protecting SSNs in the public sector, and in response, some of these vulnerabilities have since been addressed by agencies. For example, in our review of government uses of SSNs, we found that some federal, state, and local agencies do not consistently fulfill the Privacy Act requirements that they inform individuals whether SSN disclosure is mandatory or voluntary, provide the statutory or other authority under which the SSN request is made, or indicate how the SSN will be used, when they request SSNs from individuals. To help address this inconsistency, we recommended that the Office of Management and Budget (OMB) direct federal agencies to review their practices for providing required information, and OMB has since implemented this recommendation.

Actions have also been taken by some federal agencies in response to our previous finding that millions of SSNs are subject to exposure on individual identity cards issued under federal auspices. [13] Specifically, in 2004, we reported that an estimated 42 million Medicare cards, 8 million Department of Defense (DOD) insurance cards, and 7 million Department of Veterans Affairs (VA) beneficiary cards displayed entire 9-digit SSNs. While the Centers for Medicare and Medicaid Services, with the largest

[13]GAO-05-59.

number of cards displaying the entire 9-digit SSN, does not plan to remove the SSN from Medicare identification cards, VA and DOD have begun taking action to remove SSNs from cards. For example, VA is eliminating SSNs from 7 million VA identification cards and will replace cards with SSNs or issue new cards without SSNs between 2004 and 2009, until all such cards have been replaced.

However, some of the vulnerabilities we identified in public sector SSN protection have not been addressed. For example, while the Privacy Act and other federal laws prescribe actions agencies must take to assure the security of SSNs and other personal information, we found that these requirements may not be uniformly observed by agencies at all levels of government.[14] In addition, in our review of SSNs in government agency-maintained public records, we found that SSNs are widely exposed to view in a variety of these records.[15] While some agencies reported taking actions such as removing SSNs from electronic versions of records, without a uniform and comprehensive policy, SSNs in these records remain vulnerable to potential misuse by identity thieves. Consequently, in both instances, we suggested 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. Some steps have since been taken at the federal level to promote inter-agency discussion of SSN protection, such as creation of the President's Identity Theft Task Force in 2006 to increase the safeguards on personal data held by the federal government.

In April 2007, the Task Force completed its work, which resulted in a strategic plan aimed at making the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. The plan's recommendations focus in part on increasing safeguards employed by federal agencies and the private sector with respect to the personal data they maintain, including decreasing the unnecessary use of SSNs in the public sector. To that end, last month, OMB issued a memorandum requiring federal agencies to examine their use of SSNs in systems and programs in order to identify and eliminate instances in which collection or use of the SSN is unnecessary. In addition, the memo requires federal agencies to participate in governmentwide

[14]GAO-02-352.

[15]GAO-05-59.

efforts to explore alternatives to agency use of SSNs as personal identifiers for both federal employees and in federal programs.

Vulnerabilities Persist in Federal Laws Addressing SSN Collection and Use by Private Sector Entities

In our reviews of private sector entities' collection and use of SSNs, we found variation in how different industries are covered by federal laws protecting individuals' personal information. For example, although federal laws place restrictions on reselling some personal information, these laws only apply to certain types of private sector entities, such as financial institutions. Consequently, information resellers are not covered by these laws, and there are few restrictions placed on these entities' ability to obtain, use, and resell SSNs. However, recently proposed federal legislation, if implemented, may help to address this vulnerability.[16] For example, the SSN Protection Act of 2007, as introduced by Representative Edward Markey, would give the Federal Trade Commission (FTC) rulemaking authority to restrict the sale and purchase of SSNs and determine appropriate exemptions.[17] The proposed legislation would therefore improve SSN protection while also permitting limited exceptions to the purchase and sale of SSNs for certain purposes, such as law enforcement or national security.

Vulnerabilities also exist in federal law and agency oversight for different industries that share SSNs with their contractors.[18] For example, while federal law and oversight of the sharing of personal information in the financial services industry is very extensive, federal law and oversight of the sharing of personal information in the tax preparation and telecommunications industries is somewhat lacking. Specific actions to address these vulnerabilities in federal laws have not yet been taken, leaving SSNs maintained by information resellers and contractors in the tax preparation and telecommunications industries potentially exposed to misuse, including identity theft.

We also found a gap in federal law addressing SSN truncation, a practice that would improve SSN protection if standardized. Specifically, in our Internet resellers report, several resellers provided us with truncated SSNs

[16]Legislation proposed in the 110th Congress that may help to address this vulnerability includes H.R. 948 "Social Security Number Protection Act of 2007," H.R. 958 "Data Accountability and Trust Act," and S.238 "Social Security Number Misuse Prevention Act."

[17]HR 948.

[18]GAO-06-238.

showing the first five digits, though other entities truncate SSNs by showing the last four digits. Therefore, because of the lack of SSN truncation standards, even truncated SSNs remain vulnerable to potential misuse by identity thieves and others. While we suggested that the Congress consider enacting standards for truncating SSNs or delegating authority to SSA or some other governmental entity to do so, SSN truncation standards have yet to be addressed at the federal level.

Concluding Observations

The use of SSNs as a key identifier in both the public and private sectors will likely continue as there is currently no other widely accepted alternative. However, because of this widespread use of SSNs, and the vulnerabilities that remain to protecting this identifier in both sectors, SSNs continue to be accessible to misuse by identity thieves and others. Given the significance of the SSN in committing fraud or stealing an individual's identity, it would be helpful to take additional steps to protect this number. As the Congress moves forward in pursuing legislation to address SSN protection and identity theft, focusing the debate on vulnerabilities that have already been documented may help target efforts and policy directly toward immediate improvements in SSN protection. To this end, we look forward to supporting the Subcommittee and the Congress however we can to further ensure the integrity of SSNs. Related to this, we have issued a report on the federal government's provision of SSNs to state and local public record keepers, and we have also recently begun a review of the bulk sale of public records containing SSNs, including how federal law protects SSNs in these records when they are sold to entities both here and overseas.

Mr. Chairman, this concludes my prepared testimony. I would be pleased to respond to any questions you or other members of the subcommittee may have.

GAO Contacts

For further information regarding this testimony, please contact me at bertonid@gao.gov or (202) 512-7215. In addition, contact points for our Offices of Congressional Relations and Public Affairs can be found on the last page of this statement. Individuals making key contributions to this testimony include Jeremy Cox, Rachel Frisk, Ayeke Messam, and Dan Schwimer.

Related GAO Products

Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs. GAO-06-495. Washington, D.C.: May 17, 2006.

Social Security Numbers: More Could Be Done to Protect SSNs. GAO-06-586T. Washington, D.C.: March 30, 2006.

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.

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