**OFFICE OF**
**THE INSPECTOR GENERAL**

**SOCIAL SECURITY ADMINISTRATION**

# STATE AND LOCAL GOVERNMENTS' COLLECTION AND USE OF SOCIAL SECURITY NUMBERS

**September 2007** **A-08-07-17086**

# AUDIT REPORT

## Mission

**By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.**

## Authority

**The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:**

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

**To ensure objectivity, the IG Act empowers the IG with:**

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

## Vision

**We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.**

# SOCIAL SECURITY

**MEMORANDUM**

Date: September 10, 2007 Refer To:

To: The Commissioner

From: Inspector General

Subject: State and Local Governments' Collection and Use of Social Security Numbers (A-08-07-17086)

## OBJECTIVE

Our objective was to assess State and local governments' collection and use of Social Security numbers (SSNs) and the potential risks associated with current practices.

## BACKGROUND

State and local governments provide programs and services to millions of individuals each year. To assist in this process, many State and local governments collect and use SSNs for various purposes. Although no single Federal law regulates overall use and disclosure of SSNs, the *Social Security Act,* the *Privacy Act of 1974*, and the *Family Educational Rights and Privacy Act*, contain provisions that govern disclosure and use of SSNs. See Appendix A for more information on the specific provisions of these laws. Additionally, the Office of Management and Budget (OMB) recently issued a memorandum to Federal agencies on safeguarding against and responding to breaches of personally identifiable information, including SSNs.[1] Federal agencies are required to reduce the volume of collected and retained personally identifiable information to the minimum necessary,[2] including establishment and implementation of plans to eliminate unnecessary collection and use of SSNs.[3] The OMB guidelines also require Federal agencies to develop and implement an appropriate policy relative to safeguarding personally identifiable information outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.[4]

---

[1] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach in Personally Identifiable Information,* May 22, 2007.

[2] OMB M-07-16, page 2.

[3] OMB M-07-16, Attachment 1, § B.2.a.

[4] OMB M-07-16, Attachment 4 § A.

We reviewed relevant laws from all 50 States to (1) discern the purposes for which SSN collection and use is legally mandated, (2) identify measures States have taken to limit SSN collection and use and (3) evaluate State laws that govern the protection of SSNs from improper use and disclosure. Because of the large number of State and local entities and associated programs throughout the United States, we focused our review on the following:

- existing State laws as previously described,
- State and local governments' posting of SSNs on Internet websites,[5]
- SSNs used for kindergarten through 12th grade (K-12) school registration and tracking,
- SSNs used in State prescription drug monitoring programs,
- cases in which State and local governments inadvertently and/or improperly disclosed SSNs, and
- measures and/or laws implemented by States or local governments that we believe represent best practices.

See Appendix B for additional details regarding our scope and methodology.

## RESULTS OF REVIEW

Based on our reviews of selected State and local governments' policies and practices, we are concerned about the collection, use and protection of SSNs by these entities. Despite the increasing threat of identity theft, some State and local governments collect and use SSNs for various purposes, even when another identifier would suffice. While Federal or State law may require that government agencies collect SSNs in some instances, we believe some do so for convenience. In our opinion, a government entity should not place more value on convenience than on the security of its constituents' personal information. We also believe individuals who provide their SSNs to government entities have an expectation that these numbers will be protected from public disclosure. Based on our previous audit and investigative findings, we know unnecessary use of SSNs increases the potential for dishonest individuals to illegitimately attain these numbers and misuse them, thus creating SSN integrity issues. Some State and local governments shared our concern regarding the protection of this sensitive personal information—and preventing improper disclosure and identity theft—and have taken steps to reduce the collection and use of SSNs.

[5] We reviewed Internet websites of all State governments. We also selected and reviewed a sample of local government and K-12 school websites because of the large number of such entities.

Given the Federal government's increased actions to safeguard SSNs, we believe SSA should seek legislation to limit State and local governments' collection and use of SSNs and improve the protection of this information when obtained. We also believe such legislation should model OMB's guidance to Federal agencies and include similar penalties or "consequences" when State or local governments/employees fail to follow these laws.

## STATE AND LOCAL GOVERNMENTS' COLLECTION AND USE OF SSNs

State and local governments collect and use SSNs for a variety of purposes. We identified instances in which they posted public documents that contained SSNs on the Internet, used SSNs for school registration and student tracking, and collected SSNs to monitor prescription drug programs.[6] In addition, the Government Accountability Office (GAO) reported that State and local government agencies frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations. Although GAO found that some government agencies had taken steps to limit the use and display of SSNs, the numbers were still available in a variety of public records held by States, local jurisdictions, and courts.[7]

### SSNs Posted on the Internet

Some State and county governments post Uniform Commercial Code (UCC) filings, property tax assessor files, motor vehicle records, registered voter files, and court filings that contain SSNs on the Internet. State and local governments routinely make documents available to the public and allow individuals to make copies at courthouses and county offices. To reduce the time employees spend pulling and copying documents for the public, some States and counties post public documents on the Internet. Unfortunately, some of these documents include individuals' SSNs that may be viewed by individuals who do not have a need to know this information.

During our audit period, 11 States were posting copies of UCC filings that included individuals' SSNs on the Internet. However, we are encouraged to report that, by the completion of our audit work, eight of these States had discontinued this practice. Some of these States redacted the SSNs from the on-line documents, and others no longer allowed users to obtain the documents on-line. Unfortunately, at the time of this report, three States still had copies of UCC filings that included individuals' SSNs on the Internet.[8] Displaying such information on the Internet allows countless individuals to

---

[6] We do not intend to imply that these are the only ways in which State and local governments collect and use SSNs.

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

[8] Maryland, Ohio and Rhode Island. In response to our draft report, the Ohio Secretary of State sent us a letter stating that her office has taken the necessary steps to assure the redaction of SSNs for current online UCC filings. In June 2007, the new administration implemented a project that will ensure the redaction of SSNs for archived, online UCC filings by September 30, 2007.

view others' SSNs, unnecessarily subjecting them to the possibility of identity theft. As such, we encourage State and local governments not to place SSNs on public documents that may be seen by others or post such documents on the Internet. Additionally, we encourage these government entities to examine their collection of SSNs and, if possible, use an alternative identifier.

## SSNs Used for School Registration and Student Tracking

Some K-12 schools require students' SSNs for school registration and use SSNs to track students throughout their school years. For example, we identified laws in three States[9] that required that schools obtain students' SSNs. Additionally, schools in 40 other States[10] collected students' SSNs at registration, even though no State law required that they do so. Schools often use SSNs as primary student identifiers to help in record keeping and to identify students when they transfer to another school or apply for college. The *No Child Left Behind Act of 2001*[11] requires that each State implement a Statewide accountability program that measures the progress of students and schools through the collection and analysis of data. However, this law does not require that States use SSNs to identify and track students. Rather, we believe some K-12 schools use SSNs as a matter of convenience. The number is unique and, in many cases, is already established to help schools track students throughout their school careers.

For the 2004/2005 school year, the National Education Association estimated that there were more than 48 million K-12 students in over 15,000 school districts across the country.[12] We believe the collection and use of SSNs without proper controls is a significant vulnerability for this young population. Recent data indicate the number of children under age 18 whose identities have been stolen is growing.[13] This is particularly troubling given that some of these individuals may not become aware of such activity until they apply for a credit card or student loan.

---

[9] Alabama, Georgia, and Tennessee.

[10] Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, Wisconsin, and Wyoming.

[11] Pub. L. No. 107-110 § 1111(b)(3).

[12] *Ranking and Estimates, June 2005.* National Education Association.

[13] According to the Federal Trade Commission, identity theft complaints from individuals under age 18 increased from 3 percent of all identity theft complaints it received in 2003 to 5 percent in 2005. *National and States Trends in Fraud and Identity Theft: January – December 2003, January 2004.* Federal Trade Commission. *Identity Theft Victim Complaint Data: January 1 – December 31, 2005, January 2006.* Federal Trade Commission.

In previous audits,[14] we assessed universities' use of SSNs as student identifiers and identified instances in which universities used SSNs as the primary student identifier or for other purposes. Numerous incidences of identity theft at colleges and universities and the recognition that SSNs are linked to vast amounts of personal information led some schools to reconsider the practice of using SSNs as primary student identifiers. Several schools took steps to reduce their reliance on SSNs or turned to alternative identifiers. In addition, some States enacted laws to regulate college and university use of SSNs. We are encouraged by these efforts and suggest that State and local governments consider affording these same protections to their youngest constituents – those in K-12 schools.

### SSNs Used to Monitor State Program

Some State and local governments collect and use SSNs to administer various programs and services. For example, we identified prescription drug monitoring programs in some States, which track individuals who obtain controlled substance prescriptions. As part of these programs, some States require that individuals who present a prescription for a controlled substance provide a unique identifying number, such as a driver's license, passport, or SSN. Kentucky policy mandates that this identifier be the individual's SSN. However, Alabama, Hawaii, Massachusetts and Indiana give individuals an option of providing an SSN or other unique number. While these programs aid law enforcement in obtaining information against suspected criminals, we believe States could rely on other unique identifying documents, such as a driver's license (which includes a photograph) to track individuals. We encourage States to use a substitute for the SSN if a personal identifier is needed to track individuals in a State program.

## POTENTIAL RISKS ASSOCIATED WITH COLLECTING AND USING SSNs

Each time an individual divulges his or her SSN, the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases. We believe the following examples illustrate individuals' risk of exposure to such activity.

- The Mississippi Secretary of State's Internet website posted over 2 million documents containing thousands of individuals' SSNs. State officials removed the link to the documents after a privacy activist filed a complaint.

- An Ohio county's website contained public documents, including traffic tickets, that contained individuals' SSNs and other personal information. Individuals involved in an identity theft ring were arrested in March 2006 for allegedly stealing nearly $500,000 with the aid of the county's website.

[14] *Universities' Use of Social Security Numbers as Student Identifiers in Regions IV and X*, December 2004 and March 2005.

- A high school in Illinois mistakenly posted SSNs and other personal information of over 2,000 students on the school's website.

- A high school in Michigan had a hard drive stolen that contained SSNs, transcripts, test scores, and addresses of students who graduated from the high school between 1994 and 2007. It is unclear how many students this may have impacted.

- A California county department of public social services disposed of documents that contained names, addresses, telephone numbers, SSNs, and medical information of an estimated 94,000 people who received services from the office over 3 years. Those documents were disposed of next to a public recycling bin.

## SOME STATE AND LOCAL GOVERNMENTS HAVE TAKEN STEPS TO LIMIT SSN COLLECTION AND USE

The increase in identity theft and the recognition that SSNs are linked to vast amounts of personal information have led some State and local governments to limit SSN collection and use.[15] We identified 11 States that have taken steps to remove SSNs from public documents[16] and 24 States that have passed laws to protect individuals' SSNs from being on public documents.[17] In addition, we identified 15 States that have passed laws to restrict companies and individuals from posting or publicly displaying SSNs,[18] printing them on cards, transmitting them over the Internet, and mailing them without safety measures. The following examples illustrate these steps.

- New Jersey prohibits individuals' SSNs on documents intended for public recording. County recording offices have the authority to remove SSNs from documents.

- California allows individuals to redact SSNs from pleadings, attachments, documents, or other written material filed with a court. Individuals are responsible for requesting the court to remove their SSN from a public document.

---

[15] We do not intend to suggest that the States discussed below are the only States that have taken steps to limit SSN collection and use.

[16] Alabama, California, Georgia, Indiana, Kansas, Nevada, New Jersey, New York, North Carolina, Ohio, and Tennessee have laws to remove SSNs from public documents if not required by Federal law.

[17] The following States have laws to protect individuals' SSNs from being on public documents: Alabama, California, Georgia, Indiana, Iowa, Kansas, Louisiana, Maine, Minnesota, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, West Virginia, and Wisconsin.

[18] The law only applies to individuals in Illinois, Maryland, Michigan, and Virginia. The law applies to both individuals and entities in Arizona, Arkansas, California, and Colorado. The law only applies to entities in Connecticut, Minnesota and Missouri. The law only applies to businesses in New Mexico and Vermont and only to employing entities in Oklahoma. In Texas, the law applies to individuals other than government or a government subdivision or agency.

- North Carolina prohibits government agencies and their representatives from collecting SSNs from individuals unless it is authorized by law or imperative for the performance of that agency's duties, as prescribed by law. Government agencies and their representatives are prohibited from intentionally communicating SSNs to the general public, printing SSNs on cards, or printing them on any material mailed to the individual unless required by Federal or State law. This law also applies to businesses.

- South Carolina prohibits SSNs that are provided in voter registration applications from being disclosed to the public.

- Alabama requires that State agencies remove SSNs before making documents public, unless the document is a lien, conviction record, or bankruptcy filing.

In February 2007, the Maricopa County Recorder's Office in Phoenix, Arizona, began redacting SSNs from 83 million public documents it had posted on the Internet.[19] County officials told us they undertook this $4.5-million project in response to identity theft concerns,[20] constituent complaints about the on-line SSN postings, and the desire to take a proactive approach in addressing this issue.[21] The recorder's office hired a contractor to perform the SSN redaction project because officials believed the increased workload would require too much additional work for office staff.[22] The county selected a contractor who could manually review each document to ensure all SSNs were removed. In fact, the county specified that each document be manually reviewed by two individuals to ensure a 99.95 percent accuracy rate. When the contractor completes the SSN redaction project in July 2007, the county plans to purchase redaction software so it can conduct its own process in the future. Under a new Arizona law, individuals who file documents with the county must remove SSNs unless Federal law requires that the number be on the document. However, county officials told us they still plan to use redaction software to ensure they do not post SSNs on the Internet in the future. While this was an expensive undertaking for Maricopa County, we applaud its actions to better secure its constituents' personal data.

We also identified instances in which K-12 schools have reduced their reliance on SSNs or turned to alternative identifiers. For example, in 2005, Arkansas passed *The Student*

---

[19] The county recorder's office began posting public records on the Internet in 1997 and included records from 1991 forward. County officials estimated that about 6 percent of the documents contained SSNs.

[20] In 2005, the Phoenix metropolitan area had the highest rate of identity theft in the nation according to the Federal Trade Commission.

[21] County officials told us they funded the SSN redaction project with fees the recorder's office received for each recorded document. According to county officials, the recorder's office did not use any of the county's general funds to pay for the SSN redaction project.

[22] County officials told us the recorder's office receives about 6,500 documents daily.

*Identity Protection Act*,[23] which prohibits schools from using, displaying, releasing, or printing a student's SSN or any part of the SSN on any report, identification card or badge, or on any document that will be made available or released to the public, to a student, or to a student's parent or guardian without express written consent except if the records are transferred to or between the Arkansas Department of Education, other public schools or school districts, or other government agencies as allowed or required by Federal law, State law, or State Board of Education rule. The Pennsylvania Department of Education recently decided to forbid school districts from requiring that students show SSNs to register. Instead, the Pennsylvania Department of Education plans to start tracking students with an assigned unique identification number to help guard against identity theft. The Alaska Department of Education and Early Development attempted and failed to use students' SSNs as their primary student identifier. The schools received approximately 60 percent of students' SSNs because many parents refused to provide the numbers. As a result, the Alaska Department of Education decided to begin assigning a 10-digit number to each K-12 child in the public schools.

## CONCLUSION AND RECOMMENDATIONS

Despite the potential risks associated with collecting and using SSNs, many State and local governments continue this practice. While we recognize SSA cannot prohibit State and local governments from using SSNs, we believe SSA should seek legislation that would limit State and local governments' collection and use of SSNs and improve protection of this information when it is obtained. We recognize that such legislation could be inconvenient for States and local governments and may initially result in a cost investment when converting current programs that use the SSN. However, given the potential threats to SSN integrity, such a challenge should not discourage SSA from seeking these measures, which will better safeguard the sensitive and personal information of numberholders.

Accordingly, we recommend that SSA:

1. Seek legislation to limit State and local governments' collection and use of SSNs and improve the protection of this information when obtained. We believe such legislation should model OMB's guidance to Federal agencies and include similar penalties or "consequences" when State or local governments fail to follow these laws.

2. Coordinate with State and local governments (for example, through national and regional governmental associations) to educate them about the potential risks associated with collecting and improperly disclosing SSNs.

[23] Ark. Stat. Ann. § 6-18-208(d).

3. Promote the best practices of State and local governments that have taken steps to limit SSN collection and use.

## AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with Recommendations 2 and 3. Although SSA disagreed with Recommendation 1, it agreed in principle with similar legislation currently under consideration by Congress.[24] We are pleased that SSA is supportive of legislation to limit State and local governments' collection and use of SSNs and improve the protection of this information when obtained. We concur that seeking additional or separate legislation would not be necessary if H.R. 3046 becomes law.

SSA also provided technical comments that we considered and incorporated, where appropriate. SSA's comments are included in Appendix C.

Patrick P. O'Carroll, Jr.

[24] On July 18, 2007, the House Committee on Ways and Means voted to approve the *Social Security Number Privacy and Identity Theft Prevention Act of 2007* (H.R. 3046), a bill to amend the Social Security Act to prevent Federal, State and local governments from displaying SSNs to the public, showing the numbers on identification tags and cards and, in most cases, selling the numbers.

# Appendices

# Federal Laws that Govern Disclosure and Use of the Social Security Number

The following Federal laws establish a general framework for disclosing and using the Social Security number (SSN).

*The Privacy Act of 1974 (the "Privacy Act")*[1]

The *Privacy Act* indicates, in part, that it is unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her SSN, unless the disclosure is required by Federal statute or is to any Federal, State or local agency maintaining a system of records in existence and operating before January 1, 1975, such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.[2] Further, under *Section 7(b) of the Privacy Act,*[3] any Federal, State, or local government agency requesting that an individual disclose his/her SSN must inform the individual whether the disclosure is voluntary or mandatory, by what statutory or other authority the SSN is solicited and what uses will be made of the SSN.

*The Family Educational Rights and Privacy Act*[4]

*The Family Educational Rights and Privacy Act (FERPA)* protects the privacy of student education records. FERPA applies to those schools that receive funds under an applicable program of the U.S. Department of Education.[5] Under FERPA, an educational institution must have written permission from the parent or eligible student to release any personally identifiable information (which includes SSNs) from a student's education record.[6] FERPA does, however, provide certain exceptions in

[1] Pub. L. No. 93-579, 5 U.S.C. 552a.

[2] Pub. L. No. 93-579 § 7(a), 5 U.S.C. 552a, note 7.

[3] Pub. L. No. 93-579 § 7(b), 5 U.S.C. 552a, note 7.

[4] 20 U.S.C. § 1232g.

[5] 34 C.F.R. Part 99, Subpart A, § 99.1.

[6] 20 U.S.C. § 1232g(b).FERPA gives parents certain rights with respect to their children's education records. 34 C.F.R. Part 99 Subpart B § 99.10(a). These rights transfer to the child when the child reaches the age of 18 or attends an institution of postsecondary education. 20 U.S.C. § 1232g(d). Children that have been transferred rights are referred to as "eligible students". 34 C.F.R. Part 99, Subpart A § 99.5(a).

which a school is allowed to disclose records without consent.[7] These exceptions include disclosure without consent to other school officials who have a legitimate educational interest in the information, to officials of institutions where the student is seeking to enroll/transfer, to parties to whom the student is applying for financial aid, to the parent of a dependent student, to appropriate parties in compliance with a judicial order or lawfully issued subpoena, or to health care providers in the event of a health or safety emergency.[8]

*The Social Security Act*

The Social Security Act provides, in part, that "Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record".[9] The Social Security Act also provides, in part, that "[w]hoever discloses, uses, or compels the disclosure of the social security number of any person in violation of the laws of the United States; shall be guilty of a felony…".[10] The Social Security Act authorizes certain State and local agencies to use the SSN for certain purposes and allows, or in certain instances requires, such agencies to require individuals to furnish their SSNs for such purposes.[11]

---

[7] 20 U.S.C. § 1232g(b)(1).

[8] 20 U.S.C. § 1232g(b)(1).

[9] 42 U.S.C. § 405(c)(2)(C)(viii).

[10] 42 U.S.C. § 408(a)(8).

[11] 42 U.S.C. § 405(c)(2)(C)(i), (ii), (v), (vi), (D) and (E).

# Scope and Methodology

To accomplish our objective, we reviewed relevant laws from all 50 States to (1) discern the purposes for which Social Security number (SSN) collection and use is legally mandated, (2) identify measures States have taken to limit SSN collection and use and (3) evaluate State laws that govern the protection of SSNs from improper use and disclosure. Because there are such a large number of State and local entities and associated programs throughout the United States, we focused our review on the following:

- existing State laws as previously described;
- State and local governments' posting of SSNs on Internet websites;[1]
- SSNs used for kindergarten through 12th grade (K-12) school registration and tracking;
- SSNs used in State prescription drug monitoring programs;
- cases in which State and local governments inadvertently and/or improperly disclosed SSNs;
- measures and/or laws implemented by States or local governments that we believe represent best practices;
- interviewed selected county officials responsible for redacting SSNs from the Internet; and
- reviewed selected studies, articles, and reports regarding State and local governments' collection and use of SSNs.

We visited one county recorder's office and interviewed officials to learn more about their SSN redaction project. In addition, we identified State and local governments, including K-12 schools, that have limited their use of SSNs and determined the reasons for this changes and best practices that could be adopted by other State and local governments. Our review of internal controls was limited to gaining an understanding of the use of SSNs by State and local governments. The Social Security Administration entity reviewed was the Office of the Deputy Commissioner for Operations. We conducted our audit from October 2006 through April 2007 in accordance with generally accepted government auditing standards.

[1] We reviewed Internet websites of all State governments. We also selected and reviewed a sample of local government and kindergarten through 12th grade school websites because of the large number of such entities.

# Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: August 23, 2007 Refer Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: David V. Foster /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, “State and Local Governments' Collection and Use of Social Security Numbers" (A-08-07-17086)--INFORMATION

We appreciate OIG’s efforts in conducting this review. Our response to the reports findings and recommendations are attached.

Please let me know if we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment

**COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "STATE AND LOCAL GOVERNMENTS' COLLECTION AND USE OF SOCIAL SECURITY NUMBERS" (A-08-07-17086)**

Thank you for the opportunity to review and comment on the draft report. As the issuer of Social Security numbers (SSN), we have been an active participant and are continuously working with Federal agencies to address issues surrounding Personally Identifiable Information (PII) breaches. We serve as a member of the President's Interagency Identity Theft Task Force whose mission is to strengthen Federal efforts to protect against the unlawful use of another person's identifying information. As part of those efforts, we are already in the process of assessing the public and private sector uses of SSNs to identify actions that will strengthen the Federal government's efforts in the fight against identity theft. We are committed to helping States reduce unnecessary collection of SSNs and to improve protections and safeguards. We believe the actions planned, or taken, as described in our responses to the specific recommendations below, help achieve those goals. We are also providing some technical comments to enhance the accuracy of the report.

Recommendation 1

The Social Security Administration (SSA) should seek legislation to limit State and local governments' collection and use of SSNs and improve the protection of this information when obtained. We believe such legislation should model the Office of Management and Budget's guidance to Federal agencies and include similar penalties or "consequences" when State or local governments fail to follow these laws.

Response

We disagree. The legislation that OIG is recommending is the subject of wider legislation currently under consideration by Congress. On July 18, 2007, the House Committee on Ways and Means voted 41-0 to approve H.R. 3046, a bill to amend the Social Security Act to prevent Federal, State and local governments from displaying SSNs to the public, showing the numbers on identification tags and cards and, in most cases, selling the numbers. We believe the bill addresses this recommendation and provides for penalties or 'consequences' when State or local governments fail to follow these laws. Seeking additional or separate legislation is not appropriate and could be counterproductive.

Recommendation 2

SSA should coordinate with State and local governments (for example, through national and regional governmental associations) to educate them about the potential risks associated with collecting and improperly disclosing SSNs.

Response

We agree. We believe more can be done to alert State and local governments to the risks of using and/or displaying SSNs on documents that are used as identifiers of the public. We (through our Office of External Affairs) will continue to use our contacts with national organizations to alert the staffs of these organizations to the risks of including SSNs on public documents and will request their help in reducing instances where SSNs are printed or displayed on computer terminals. We will also continue to make the public aware, through SSA public information materials and news articles placed in local print media, of the problems associated with the misuse and over utilization of SSNs.

Recommendation 3

SSA should promote the best practices of State and local governments that have taken steps to limit SSN collection and use.

Response

We agree. As part of our efforts described for recommendation number 2, we will identify and promote the best practices used by those public entities that find ways to limit the use of SSNs in conducting their routine business with the public.

# OIG Contacts and Staff Acknowledgments

## *OIG Contacts*

Kimberly Byrd, Director, Southern Audit Division, (205) 801-1650

Jeff Pounds, Audit Manager, (205) 801-1606

## *Acknowledgments*

In addition to those named above:

Hollie Reeves, Auditor

Neha Smith, Senior Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-08-07-17086.

# DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

# Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

## Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

## Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

## Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

## Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.