SOCIAL SECURITY

Inspector General

August 22, 2003

The Honorable E. Clay Shaw, Jr.
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives
Washington, D.C. 20515

Dear Mr. Shaw:

In response to your July 21, 2003 questions related to the July 10th *Hearing on Use and Misuse of Social Security Numbers*, I am pleased to provide you with information on issues related to the Social Security number (SSN).

The enclosed report provides information regarding the following:

- enumeration;
- electronic verification of SSNs;
- enhancement of civil and criminal remedies;
- provisions for statutory authority to share information with law enforcement partners; and
- funding resources for activities related to combating identity theft or SSN misuse.

If you have any questions or would like to be briefed on this issue, please call me or have your staff contact H. Douglas Cunningham, Executive Assistant, at (202) 358-6319.

Sincerely,

James G. Huse, Jr.

Enclosure

cc:
Jo Anne B. Barnhart

CONGRESSIONAL RESPONSE REPORT

Use and Misuse of the Social Security Number

A-03-03-24048

August 2003

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

Background

In response to a July 21, 2003 request from the Chairman of the Subcommittee on Social Security, and following a July 10th *Hearing on Use and Misuse of Social Security Numbers,* we are providing the enclosed report which contains information related to:

- enumeration,[1]
- electronic verification of Social Security numbers (SSN),
- enhancement of civil and criminal remedies,
- provisions for statutory authority to share information with law enforcement partners, and
- funding resources for activities related to combating identity theft or SSN misuse.

TESTIMONY ON USE AND MISUSE OF THE SSN

On July 10, 2003, the Inspector General (IG) of the Social Security Administration (SSA) testified before the House Ways and Means Committee, Subcommittee on Social Security. In that testimony, the IG noted that the Nation needs to protect the SSN at three stages: upon issuance, during the life of the numberholder, and following the numberholder's death. The IG stated:

- At Stage One, the Office of the Inspector General (OIG) is working closely with the Subcommittee and SSA to strengthen controls over the enumeration process, ensure the integrity of identification documents, and make it as difficult as possible to fraudulently obtain an SSN from the Government.

- At Stage Two, where the OIG has focused most of its efforts, the Office has made the most progress. In the last several years, we have conducted numerous audits and made sweeping recommendations to SSA to improve the SSN misuse problem in the earnings reporting process, and most importantly, to improve controls over SSN misuse as it pertains specifically to Homeland Security.

- Stage Three, following the death of the numberholder, is an area in which the OIG is working hard to ensure that, through timely reporting, appropriate cross-matching, and better controls, the SSNs of deceased individuals are not recycled for inappropriate purposes.

[1] Enumeration is the process of assigning and issuing SSNs to individuals.

Results of Review

The Chairman of the Social Security Subcommittee requested we respond to 13 questions. We have provided the responses in the section below.

Question #1: *Under current law, the Social Security Administration (SSA) requires proof of identity, age, and U.S. citizenship or immigration status to obtain a Social Security number (SSN) or file for benefits. However, SSA does not require photo identification to obtain an SSN or file for benefits, correct? Would you say this is a vulnerability in the application process that should be fixed?*

Answer to Question #1: You are correct, SSA does not require photo identification to obtain an SSN or file for benefits. Although we recognize the value of photo identification, we are unaware of any evidence to support the premise that photo identification has a higher probative value than other forms of identification. Individuals who present fraudulent identity documents can easily obtain fraudulent photo identification documents as well. Absent baseline photo identification with biometric attributes, it is difficult to ensure photo identification will provide greater assurance that individuals are who they say they are. In addition, there are segments of the population who legitimately do not have photo identification. For example, young children and individuals who do not drive may have no need for photo identification. Also, individuals who are victims of theft or catastrophic events (for example, fires and floods) may not have photo identification documents and need their SSN to obtain new ones.

SSA is conducting a pilot study to determine whether the Agency should change the requirements for identity documentation related to SSN assignment. For example, SSA will examine the efficacy of requiring two identity documents when an individual does not have photo identification. Preliminary results indicate that over 70 percent of applicants present photo identification documents. SSA is also conducting a pilot study wherein it will request photo identification from individuals filing for Title II and XVI disability benefits. In addition, SSA will require that individuals allow the Agency to take their photographs and make these photographs a part of their disability claims folder. SSA is conducting this pilot to determine whether photo identification will strengthen the integrity of the disability claims process by helping ensure the individual filing an application is the same individual examined by the consultative examination physician. This pilot is scheduled to run through November 2003. SSA will evaluate the results of the pilot and expand or modify its procedures accordingly.

Question #2: *In your testimony, you say that SSA should limit the number of replacement SSN cards that are issued to an individual. How should replacement cards be limited in your review?*

Answer to Question #2: In our September 2001 report, *Replacement Social Security Number Cards: Opportunities to Reduce the Risk of Improper Attainment and Misuse* (A-08-00-10061), we stated we believed the potential for individuals to improperly obtain and misuse replacement SSN cards was significant based on our work at SSA field offices and analysis of national data. Accordingly, we recommended that SSA develop regulations and incorporate appropriate system controls to limit the number of replacement SSN cards. To address extraordinary circumstances that warrant exceptions (for example, the homeless population), we recommended that SSA require management approval.

SSA has drafted regulations limiting the number of replacement SSN cards issued to individuals to 2 per year, with a lifetime limit of 10. We support this legislative proposal.

Question #3: *In your testimony, you say that SSA should require better cross-verification of records in the enumeration at birth process. Vulnerabilities in this method of SSN issuance are particularly important, because over two-thirds of new SSNs are issued this way. Could you elaborate on the vulnerabilities your office has found with the enumeration at birth process? What action, if any, has SSA taken to address this vulnerability? How would you suggest this issue be addressed?*

Answer to Question #3: In our September 2001 report, *Audit of Enumeration at Birth Program* (A-08-00-10047), we found that birth registration data provided to SSA by the test hospitals and State Bureaus of Vital Statistics (BVS) were generally accurate and reliable. However, we identified weaknesses in controls and operations that we believed SSA needed to address to reduce the enumeration at birth (EAB) program's vulnerability to potential error and misuse and to enhance program efficiency. Accordingly, we recommended that SSA re-invest some of the savings realized by the EAB program and provide necessary funding, during future contract negotiations, for the BVSs to perform periodic, independent reconciliations of registered births with statistics obtained from hospitals' labor and delivery units and periodically verify the legitimacy of sample birth records obtained from hospitals. In addition, we recommended that SSA enhance its duplicate record detection and prior SSN detection routines to provide greater protection against the assignment of multiple SSNs. We plan to start a follow-up review of the EAB program in Fiscal Year (FY) 2004 which, once completed, we can share with you and your staff.

According to SSA's EAB Project Director, contracts renegotiated in December 2002, which became effective on January 1, 2003, did not include language that required that States reconcile registered births with statistics from hospital labor and delivery units. SSA has had several discussions with the National Association of Public Health Statistics and Information Systems (NAPHSIS) regarding the most cost-effective method of reconciling births with statistics from hospitals and verifying the legitimacy of sample birth records. SSA and NAPHSIS have been unable to agree on a viable method of addressing this issue, primarily because of financial considerations. Regarding our recommendation on duplicate record detection, SSA has looked at the detection routines and practices to determine whether there are feasible software

modifications to the Automated Enumeration Screening Process that would provide greater protection. However, SSA has made no decisions to implement changes at this time.

Question #4: *Several witnesses testified about use of the SSNs of young children to commit identity theft. Please provide any statistical information you can obtain regarding the extent to which this occurs and is prosecuted. Is it usually a family member who commits identity theft using a child's SSN, or an unrelated person? Would it be advisable to stop issuing SSNs to children prior to when they start working?*

Answer to Question #4: We queried our systems to obtain statistical information pertaining to the use of children's SSNs, specifically, to determine the extent to which these SSNs are used in identity thefts and later prosecuted. We also attempted to determine whether it is usually a family member who commits identity theft using a child's SSN, or an unrelated person. Unfortunately, the information requested cannot be retrieved electronically.

Regarding the matter of not issuing an SSN until an individual starts working, it would be inadvisable, as well as impractical, to cease the practice of issuing SSNs to children at birth. For example, the Internal Revenue Service (IRS) requires that parents provide an SSN when claiming children as dependents. Furthermore, children need an SSN to obtain benefits, such as in cases where a parent dies, and when a child becomes disabled.

Question #5: *The witness for the Identity Theft Resource Center recommended creation of a Death Master File that contains every death, as well as a file with minors' names, dates of birth and SSN, to be given to credit agencies to help prevent identity theft based on those SSNs. He also recommended restricting the publication of SSNs (including those of deceased individuals) on websites. What are your thoughts on these issues?*

Answer to Question #5: Protection of the integrity of the SSN is one of our most important missions. As I stated in my testimony before this Subcommittee, "Perhaps the most important step we can take in preventing SSN misuse is to limit the SSN's easy availability."

In both our audit work and criminal investigations, we have seen the use of a deceased individual's SSN for fraudulent purposes. As I also said in my testimony, "…we are working hard to ensure that, through timely reporting, appropriate cross-matching, and better controls, the SSNs of deceased individuals are not recycled for inappropriate purposes." Therefore, we support any protection of the SSN, including the restriction of its publication on websites where the general public would have access.

Regarding the proposal for the creation of a Death Master File that would contain every death, as well as the creation of a file with minors' names, dates of birth and SSNs, we are proponents of the ability to cross-verify an individual's SSN. This is an important

tool in the fight against SSN misuse. We have submitted legislative proposals to allow the OIG to verify SSNs for law enforcement, currently being performed through a Memorandum of Understanding with SSA, and to provide SSA information to law enforcement in a life-threatening situation. We do have concerns about the creation of a file with minors' names, dates of birth and SSNs. The potential misuse of such a central file without adequate privacy controls could far outweigh its usefulness. Such a file should be created only with rigid safeguards, with consequences for those who improperly release or use its information. We urge that the creation of such a file be done carefully and with due diligence to protecting the rights of the minors.

While providing this information to credit agencies should help prevent identity theft, we believe law enforcement should also have access to the databases. As I stated above, cross-verification of an SSN is an important tool in the fight against SSN misuse. These databases would provide a wealth of vital information to law enforcement in their daily fight against crime.

Question #6: *Knowing that we cannot eliminate the use of the SSN, your staff has worked tirelessly to protect SSNs upon issuance, during the life of the numberholder, and even after the numberholder's death. Central to that process, you emphasized in your testimony that Congress should consider requiring cross-verification of SSNs throughout both governmental databases (including the SSA's) and the financial sector. Are you talking about a new database, or are you suggesting that existing verification processes be used to better advantage? How would this limit the spread of false identification and SSN misuse?*

Answer to Question #6: We are not suggesting a new database of SSNs, but rather better use of existing verification processes. We believe matching the names and SSNs in SSA's records to those of Federal and State agencies, employers, and legitimate private sector entities is one way to ensure the integrity of the SSN as well as the reliability of information in all databases. SSA's verification programs, such as the Employee Verification Service (EVS) for employers, are a key part of this process. In fact, SSA plans to place its employer verification system on-line to increase employer participation. This program, called the Social Security Number Verification Service (SSNVS), is being piloted. SSA is also piloting an SSN verification program for private companies since, as we noted in our testimony, the Patriot Act requires that the Department of the Treasury develop a system for domestic financial institutions to verify the identities of foreign nationals seeking to open accounts with information held by Federal agencies.

SSA has other completed and ongoing pilots that offer examples of better data sharing between the Agency and private sector. For example, we recently reported on the SSN Feedback Pilot, an experiment between SSA and the Office of Child Support Enforcement to verify employee data through the W-4 reporting process. In an April 2003 Congressional Response Report: *Review of the Social Security Number Feedback Pilot Project* (A-03-03-13017), we noted that the final evaluation of the pilot stated that the SSN Pilot feedback to employers improved the timeliness of employer corrections

as well as the accuracy of information used by both the Government and private sector. The report estimates employers were notified of name and SSN mismatches 12 to 18 months earlier than under the regular wage reporting process at SSA. In addition, the report noted that the SSN Pilot increased the annual wage reporting accuracy of the SSN Pilot employers by approximately 10 percent. SSA also has an ongoing pilot with the Bureau of Citizenship and Immigration Services assisting employers with both SSN verification and immigration status.

SSA also allows other Federal and State entities, such as State motor vehicle agencies, the Department of Education, State Temporary Assistance for Needy Families agencies, the Department of Veterans Affairs, prisons, and State unemployment agencies to match their data against SSA's SSN information. It is the responsibility of these non-SSA parties to make the necessary corrections to their own records to ensure the integrity of their data.

Even with these projects underway, more can be done. Our September 2002 report on EVS for registered users, *The Social Security Administration's Employee Verification Service for Registered Employers* (A-03-02-22008), noted that only 392 of approximately 6.5 million employers in the United States used SSA's EVS in the last 3 years. We also noted that SSA did not disclose pertinent information that could have assisted users. Specifically, SSA did not inform employers when a submitted SSN belonged to a deceased individual or when the SSN was issued to the individual for nonwork purposes. SSA has stated it intends to modify both EVS and SSNVS to disclose the pertinent information to employers.

We believe this cross-verification improves the integrity of SSN data, reduces improper payments, and detects and deters SSN misuse before it can become more widespread. Greater reliance on data matching should also lead to fewer opportunities for identity theft.

Question #7: *How is SSA doing in ensuring the accuracy of its databases? Are they making this a system priority? Have they incorporated information from the Death Master File into all SSN verification processes? If not, when will this be done?*

Answer to Question #7: We have previously issued several audit reports related to the accuracy of the Death Master File (DMF)—which contains approximately 69 million records—and noted it relies on two types of recordkeeping. First, the DMF does not contain every deceased SSN holder and therefore the absence of a particular person in the DMF is not necessarily proof the person is alive, as we discussed in our July 2000 audit report, *Improving the Usefulness of Social Security Administration's Death Master File* (A-09-98-61011). Second, the DMF contains the SSNs of individuals who are not actually deceased, as we discussed in our June 2001 audit report, *Old-Age, Survivors and Disability Insurance Benefits Paid to Deceased Auxiliary Beneficiaries* (A-01-00-20043). Furthermore, an academic research study, *Social Security Bulletin, The Social Security Administration's Death Master File: The Completeness of Death Reporting at Older Ages*, Vol. 64, No. 1, 2001/2002, concluded that the File's

completeness varies significantly based on the age of the decedents. The results were that death reporting for individuals age 65 or older was over 95 percent complete. However, the DMF contained only 42 percent of deaths for deceased individuals under age 25 and 74 percent for those ages 25 to 54.

In September 1999, SSA contracted with NAPHSIS to develop standards and guidelines for a Nation-wide Electronic Death Registration (EDR) system, including the on-line verification of SSNs. This system would enable SSA to receive death reports within 5 days of death and 24 hours of receipt in the State BVSs. This system would automate the death registration process and enable SSA to receive more timely and accurate death reports, resulting in significant program and workyear savings. In addition, EDR provides the infrastructure for other Federal and State agencies that rely on such information to detect and prevent erroneous payments to deceased individuals.

However, SSA needs to implement a number of systems modifications to realize the benefits of EDR. Furthermore, SSA needs to encourage State BVS agencies to establish EDR systems. SSA agreed to obtain systems support for EDR and stated that implementation is scheduled for September 2003. At that time, SSA expects to be able to process records from State BVS agencies that implement EDR systems. However, full implementation with 90 percent of the States participating will not occur until 2005 or later. Consequently, SSA also agreed to continue to work with NAPHSIS to develop and implement EDR and stated it had awarded contracts in September 2002 to New York City, South Dakota, Montana, and Minnesota.

Finally, a review of SSN verification programs indicates that not all of these programs have been updated to include information from the DMF. As noted in our response to Question #6 above, SSA had not incorporated the DMF into EVS for registered employers, though the Agency has plans to do so. Furthermore, not all of the State motor vehicle agencies that verify their data against SSA are receiving information on SSNs that belong to deceased individuals. We believe that providing entities with this information during the verification process assists both SSA and the verifying entity with data integrity. If the individual being verified is deceased, a new document will not be issued under that SSN. However, if the individual being verified is incorrectly shown as deceased on Agency records, the alert to the verifying entity should cause the individual to contact SSA so the information can be corrected.

Question #8, Part I: *You mentioned in your testimony that we need enhanced penalties for SSA employees who assist criminals in obtaining SSNs. Could you describe cases you have worked on?*

Answer to Question #8, Part I: Typically, SSA employees who assist individuals in illegally obtaining SSNs will enter into the SSA system to issue an SSN that has not been previously assigned to an individual. For a fee, the SSA employee provides the SSN to a third party (or middleman) who then resells the SSN. This provides the ultimate recipient of the SSN with a unique SSN not associated with another person or the recipient.

Question #8, Part II: *What penalties applied under current law?*

Answer to Question #8, Part II: Depending on the individual facts as well as the decision of the prosecuting Assistant United States Attorney (AUSA), examples of potential penalties include, but are not limited to, a violation of

1. section 208 of the Social Security Act, 42 U.S.C. § 408, which carries a penalty of up to 5 years in prison and/or a fine under title 18 of the United States Code;

2. 18 U.S.C. § 371, which carries a penalty of up to 5 years in prison and/or a fine under title 18 of the United States Code; or

3. 18 U.S.C. § 201, which carries a penalty of up to 15 years and/or a fine under title 18 of the United States Code or not more than three times the monetary equivalent of the thing of value.

Question #8, Part III: *What additional penalties are needed?*

Answer to Question #8, Part III: Under the current statutes cited above, there is no minimum sentence. As a result, under the current sentencing guidelines, SSA employees convicted of selling hundreds of SSNs are receiving only months in jail or no jail time at all, only probation. Three examples include the following.

1. A former Service Representative sentenced to 3 years' probation and community service after pleading guilty to a bribery charge in connection with issuing 100 to 200 Social Security cards to illegal aliens. The Service Representative received between $50 and $150 for each card.

2. A former Service Representative was convicted of selling approximately 300 SSNs to illegal aliens over a 4-year period, receiving $400 for each number/card. The Service Representative received 3 years' probation and was fined $2,000.

3. A former Service Representative admitted to processing "hundreds" of fraudulent SSN cards, receiving $100 to $200 for each card. The Service Representative was sentenced to 4 months in jail and 3 years' probation.

The additional penalties we seek will structure the penalties based on the severity of the SSA employee's actions, providing for a minimum sentence. SSA employees issuing SSNs are in a position of trust. When this trust is violated, the effect on SSA's programs and operations and on the public in general can be devastating. Fortunately, the number of SSA employees taking part in these crimes is small. However, these crimes strike at SSA's core mission. Participation in such crimes cannot be tolerated.

The proposed penalty structure is as follows:

1. imprisonment not less than 1 year and up to 5 years and a fine under title 18 of the United State Code for the fraudulent sale or transfer of not more than 50 Social Security account numbers and/or Social Security account number cards;

2. imprisonment not less than 5 years and up to 10 years and a fine under title 18 of the United State Code for the sale or transfer of more than 50, but not more than 100 Social Security account numbers and/or Social Security account number cards; or

3. imprisonment not less than 10 years and up to 20 years and a fine under title 18 of the United State Code for the sale or transfer of more than 100 Social Security account numbers and/or Social Security account number cards.

Question #9, Part I: *You mentioned in your testimony that we need civil monetary penalties for SSN misuse, since criminal prosecution is not always available for SSN misuse and other Social Security-related crimes. In what cases is criminal prosecution not pursued?*

Answer to Question #9, Part I: Because of the volume of cases in some Districts, the U.S. Attorney's office has instituted a minimum loss requirement to pursue a case either criminally or civilly. Depending on the office, this requirement could be from $10,000 to $100,000 or higher for fraud cases. Under section 1129 of the Social Security Act, 42 U.S.C. § 1320a-8, the U.S. Attorney must prosecute or decline the case criminally and decline the case civilly before we may proceed.

As an example, if the minimum loss requirement is $50,000 in the U.S. Attorney's office and the Social Security-related loss is $30,000, without some other compelling reason to prosecute the case, for example the accused is a public official, the U.S. Attorney's office will usually decline to prosecute the case criminally and civilly. In addition, if the potential defendant is sympathetic in some regard, an AUSA may decline to prosecute them criminally.

In addition, the civil monetary penalties we are seeking would expand the scope of section 1129. Currently, the section applies only to false statements or misrepresentations of a material fact in relation to an individual's right to receive benefits or the amount of benefits under the Social Security Act. Our legislative proposals would provide us with the tools to pursue civil monetary penalties for the misuse of the SSN in cases where Social Security benefits were not involved, thus providing more support for U.S. Attorneys. This is an important step if we are serious about protecting the integrity of the SSN.

Question #9, Part II: *Why is it sometimes a better course of action to obtain punishment through civil monetary penalties?*

Answer to Question #9, Part II: Civil monetary penalties may be imposed against an individual who improperly receives Social Security benefits without subjecting the individual to potential prison time for a criminal conviction or the stigma of a criminal conviction. Particularly if the individual does not have a criminal record, this can be a viable alternative to a criminal prosecution. This resolution will reverberate throughout the community and could make someone who was contemplating doing the same thing think twice. Ability to impose a civil monetary penalty shows that, while the individual may not be criminally prosecuted, they will be responsible for their fraudulent actions.

Question #10, Part I: *You mentioned in your testimony that current law providing criminal penalties designed for crimes involving SSNs or SSN cards is not enough, because it does not provide for punishment for SSN misuse itself. During the General Accounting Office's testimony, they showed us examples of how agents used fraudulent documents to obtain SSNs and how they used fraudulent SSN cards and other documents to obtain driver's licenses. How would these crimes be punishable under current law?*

Answer to Question #10, Part I: The ultimate decision on which statute to proceed under rests with the applicable U.S. Attorney. Under the factual situation as you have described, the perpetrator of the fraud could potentially be prosecuted under sections 208(a)(6) and (a)(7)(A) of the Social Security Act, 42 U.S.C. § 408(a)(6) and (a)(7)(A). It is a violation of section 208(a)(6) of the Social Security Act, 42 U.S.C. § 408(a)(6), for an individual to furnish false information to set up their account with SSA, including receipt of an SSN.

It is a violation of section 208(a)(7)(A) of the Social Security Act, 42 U.S.C. § 408(a)(7)(A) to "willfully, knowingly, and with intent to deceive," use an SSN acquired by providing false information to SSA.

Violators of either section may be fined under title 18, U.S.C., and/or imprisoned for not more than 5 years.

In addition, if an SSA employee takes part in the crime, by fraudulently providing an SSN to the individual, knowing the information was false, the SSA employee may be guilty of aiding and abetting, punishable as if a principal. The SSA employee may also potentially be charged under 18 U.S.C. § 371, the *Conspiracy to Commit Offense or to Defraud United States*. Finally, if money or something of value changed hands, both the SSA employee providing the SSN and the individual receiving the SSN may be guilty of violating 18 U.S.C. § 201, *Bribery of Public Officials and Witnesses*.

Question #10, Part II: *How would the changes you propose make it possible, or at least easier, to punish these crimes?*

Answer to Question #10, Part II: As stated in my testimony, the changes "must provide meaningful criminal penalties in the Social Security Act, must provide enhanced penalties for those few SSA employees who betray the public trust and assist criminals

in obtaining SSNs, and must provide an administrative safety net in the form of Civil Monetary Penalties to allow some form of relief when criminal prosecution is not available for SSN misuse and other Social Security-related crimes."

As discussed in more detail in Questions 8, 9 and 12, we have submitted several proposals in this area. One proposal would enhance criminal penalties for SSA employees who assist criminals in obtaining SSNs. This proposal is designed to provide mandatory minimum sentences for SSA employees based on the number of SSNs and/or Social Security cards they have provided to criminals.

In addition, we have submitted a proposal to enhance the penalties for violations of section 208 of the Social Security Act, 42 U.S.C. § 408 involving an SSN and/or Social Security card for repeat offenders and those who used the SSN and/or Social Security card for terrorism, a crime of violence, or trafficking in drugs.

The third proposal would expand the current authority under section 1129 of the Social Security Act, 42 U.S.C. § 1320a-8 to include the criminal provisions of section 208 of the Social Security Act, 42 U.S.C. § 408, as well as the legislative proposals regarding SSA employees, an individual selling their own SSN for fraudulent purposes, and assisting another person to improperly obtain a second SSN or a number that purports to be an SSN. This proposal provides an administrative safety net, allowing us to pursue the violators administratively when criminal and civil prosecution may not be available through a U.S. Attorney's office.

Question #10, Part III: *Could you give examples of cases to clarify how current law fails to adequately punish SSN misuse?*

Answer to Question #10, Part III: One area is where an individual sells his or her own SSN for fraudulent purposes. We believe the individual could potentially be prosecuted for aiding and abetting a crime or under 18 U.S.C. § 371, *Conspiracy to Commit Offense or to Defraud United States*. However, there have been several cases where the U.S. Attorney was reluctant to pursue the criminal prosecution of an individual for selling his or her own SSN.

Question #11, Part I: *Witnesses at the hearing testified about how identity thieves may repeatedly use a victim's information to open bank accounts, get credit, or commit crimes. Current law does not provide for more severe penalties for repeat SSN misuse offenders, correct?*

Answer to Question #11, Part I: Section 208 of the Social Security Act, 42 U.S.C. § 408 provides for a penalty of up to 5 years for a violation of the section. It does not provide enhanced penalties for repeat offenders or those who use SSNs in connection with drug trafficking, a crime of violence, or terrorism.
18 U.S.C. § 1028(a)(7) provides for a penalty for knowingly transferring or using, without lawful authority, the means of identification of another person. The penalty for violating this statute is not more than 15 years' imprisonment and/or a fine if the means of

identification was used to obtain item(s) of value totaling over $1,000 during any 1-year period. If the offense is committed after a prior conviction under this statute has become final, the penalty is up to 20 years' imprisonment and/or a fine.

Question #11, Part II: *What enhanced penalty structure would you suggest for repeat offenders, or for those who use SSNs in connection with drug trafficking, a crime of violence, or terrorism?*

Answer to Question #11, Part II: We would suggest the following enhanced penalty structure for violations of section 208 of the Social Security Act, 42 U.S.C. § 408.

1. If the SSN is used to facilitate an act of international and/or domestic terrorism, up to 25 years.

2. If the SSN is used to facilitate drug trafficking or in connection with a violent crime, up to 20 years.

3. After a prior offense under this section, up to 10 years.

4. Leave the rest of the violations at the current punishment, up to 5 years.

Question #11, Part III: *Is there precedent in current law for such enhanced penalties?*

Answer to Question #11, Part III: Yes. 18 U.S.C. § 1028, *Fraud and Related Activity in Connection With Identification Documents and Information*, provides for enhanced penalties for a conviction involving a prior offense, terrorism, a crime of violence or to facilitate drug trafficking. The initial punishment for a violation under § 1028 is a fine under this title and either imprisonment for not more than either 3 years or 15 years, depending upon the facts. Under 18 U.S.C. § 1028(b)(3) and (4) state:

> (3) a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed—
>
> (A) to facilitate a drug trafficking crime (as defined in section 929(a)(2));
>
> (B) in connection with a crime of violence (as defined in section 924(c)(3)); or
>
> (C) after a prior conviction under this section becomes final.
>
> (4) a fine under this title or imprisonment for not more than 25 years, or both, if the offense is committed to facilitate an act of international terrorism (as defined in section 2331(1) of this title);

18 U.S.C. § 1030, *Fraud and Related Activity in Connection With Computers*, provides enhanced penalties for a subsequent conviction. Specifically, 18 U.S.C. § 1030(3)(A) and (B) state:

> (c) The punishment for an offense under subsection (a) or (b) of this section is—

(3) (A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this section;

Question #11, Part IV: *What do you think of the Identity Theft Resource Center's suggestion to provide enhanced penalties for stealing a child's identity?*

Answer to Question #11, Part IV: We support enhanced penalties for those who perpetrate identity theft. We have submitted a legislative proposal to enhance penalties for SSA employees who assist criminals in obtaining SSNs (see Question #8 above) as well as a legislative proposal to enhance the penalty structure for violations under section 208 of the Social Security Act, 42 U.S.C. § 408. (See Question #10 above.)

We agree those less able to protect themselves should be provided additional protections. The proposal by the Identity Theft Resource Center for an enhanced penalty for anyone who commits child identity theft has merit. We would offer to work with the Subcommittee as to what the enhanced penalty should be.

Question #12, part I: *In your testimony you mentioned that the Commissioner has ad hoc authority to permit sharing of SSA information with law enforcement and requested that the SSA IG be given statutory authority to share SSA information with law enforcement partners when disclosure is necessary to protect lives, without prior authorization from the Commissioner. Please elaborate on the circumstances under which the SSA IG would release information according to this proposal?*

Answer to Question #12, part I: 20 C.F.R. § 401.195 provides that the Commissioner of SSA, or his or her designee, may disclose information if not prohibited by Federal law. The example provided in the regulation is the disclosure of information necessary to respond in a life-threatening situation. This designation is on an ad hoc basis.

Shortly after September 11, 2001, the then acting Commissioner of Social Security, pursuant to this regulation, designated me to provide such information to law enforcement in terrorist investigations. In addition, during the Washington area sniper investigation, when law enforcement officers requested help from our Special Agents, this regulation provided us with the authority to respond.

Our legislative proposal codifies this authority in the OIG within a limited scope. It would apply only to the disclosure of SSA information to respond to a life-threatening situation. As with the current designation, the ultimate responsibility as to when to disclose rests with the IG.

The proposal also requires that the IG advise, within a reasonable time, the Commissioner of SSA or his or her designee each time disclosure is made pursuant to this legislation. In addition, an annual report must be filed with the Committee on Ways and Means of the House of Representatives and the Senate Finance Committee setting forth each disclosure made during the previous FY.

During an investigation involving a life-threatening situation, time is of the essence. The time lost securing the needed authorization can mean the difference between success or failure in locating the subject and/or victim. This delay can be lengthened if the information is needed after hours or during a weekend.

This legislative proposal will save precious time when a life can be in the balance. Our proposal will allow us to assist Federal, State and local law enforcement officers in a timelier manner. We believe we have shown we are responsible in our disclosure policy and would not abuse this authority.

Question #12, Part II: *Do other Inspectors General have authority similar to what you are requesting?*

Answer to Question #12, Part II: We are not aware of any other IG with similar authority. We would point out that we are aware of no other IG with access to databases with as much information as the SSA databases, except for perhaps databases at the IRS.

Question #12, Part III: *Please cite examples of how having this authority would have helped.*

Answer to Question #12, Part III: There have been two instances of missing children in which the OIG was contacted by law enforcement to provide information. In the first instance, a local police department advised OIG of the murder of a child for the insurance benefits. The police department went on to advise that the suspect had taken out an insurance policy on another child and expressed its concern that the suspect, whose whereabouts were unknown, intended to murder the second child. The police department requested the SSN for the child to contact the National Insurance Bureau and locate the suspect via the address on the policy.

In the second instance, a child was reported missing in an area near a Social Security office. Law enforcement officers requested assistance in identifying individuals who may have been at the Social Security office.

Question #13: *What level of administrative funding does the SSA Inspector General receive for activities related to combating identity theft or SSN misuse? What types of activities are supported by this funding? Is this level of funding sufficient?*

Answer to Question #13: The OIG does not receive funding designated to be expended for specific initiatives. However, we can estimate the level of expenditures incurred by initiative. During FY 2002, approximately $10 million or 13 percent of our appropriation was dedicated to combating SSN misuse. For FY 2003, we expect to expend the same percentage of our appropriation in this effort.

The OIG conducts a number of activities related to combating identity theft and/or SSN misuse, including examining in detail the operations of SSA's enumeration business process, and applies the lessons learned from investigative casework in analyzing threats and vulnerabilities. These audit reports address various issues, including how SSA manages the enumeration business process and ensures SSA takes appropriate steps to address vulnerabilities. The OIG also produces reports from its analysis of the Annual Wage Reporting business process. Since the SSN is used as the identifier in this process, and millions in incoming wages cannot be matched to the name and/or SSN on SSA's records, key Homeland Security issues are brought forth by this process.

The OIG's investigative efforts related to SSN misuse focuses primarily on identifying those who attempt to obtain or use false or fraudulent SSNs. Determining the intent for which the number is sought is the predominant factor as to whether the investigation is considered part of our Homeland Security program. Investigations generally falling into this category include operations worked in conjunction with, or under the direction of, Offices of the United States Attorney's Joint Terrorism Task Forces at airports, power plants, and other critical infrastructures as well as activities with Foreign Terrorist Tracking Task Forces. It also includes cases involving the misuse of SSNs by (1) legal or illegal aliens whose motives for being in the United States are suspect; (2) extremist groups in this country who are intent on disrupting Federal activities; or (3) U.S. citizens who are sympathetic to foreign causes and attempt to gain or produce identity documents bearing SSNs to conceal the true identity of others.

The OIG also performs legal and legislative work to use and strengthen the legal tools available for defense of the SSN. This will continue to include a proactive role in advocating measures to enhance SSN integrity.

We also perform outreach work to support our advocacy to increase public awareness of the broad issues surrounding SSN integrity.

To augment our efforts at combating SSN misuse and identity theft, in our FY 2002 budget request, we introduced the concept of the OIG Social Security Number Integrity Protection Team. This integrated model combines the talents of auditors, criminal investigators and attorneys in a comprehensive approach allowing SSA and the OIG to effectively address this ever-increasing problem and provide assistance to SSA, Congress, the public, and other law enforcement agencies. Although funds were not appropriated to support this concept for FYs 2002 and 2003, the FY 2004 budget includes $2.2 million to fund the hiring of additional staff and support costs for the first year of a 5-year implementation period.

Appendices

Appendix A – *Acronyms*

Appendix B – *Scope and Methodology*

Appendix C – *Prior Office of the Inspector General Reports*

Acronyms

AUSA	Assistant United States Attorney
BVS	Bureau of Vital Statistics
DMF	Death Master File
EAB	Enumeration at Birth
EDR	Electronic Death Registration
ESF	Earnings Suspense File
EVS	Employee Verification Service
FY	Fiscal Year
IG	Inspector General
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service
MEF	Master Earnings File
NAPHSIS	National Association of Public Health Statistics and Information Systems
OIG	Office of the Inspector General
SSA	Social Security Administration
SSN	Social Security Number
SSNVS	Social Security Number Verification Service
TY	Tax Year

Scope and Methodology

We limited our review to summarizing prior Office of the Inspector General and Social Security Administration work regarding Social Security number misuse. We focused mainly on past results of Office of the Inspector General audits and investigations. We conducted our review in accordance with the Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency.

Prior Office of the Inspector General Reports

Social Security Administration, Office of the Inspector General Reports Related to Social Security Number Integrity		
Common Identification Number	***Report Title***	***Date Issued***
A-03-03-13017	*Congressional Response Report: Review of the Social Security Number Feedback Pilot Project*	April 2003
A-09-03-23067	*Congressional Response Report: The Social Security Administration's Efforts to Process Death Reports and Improve Its Death Master File*	January 2003
A-09-02-22023	*Effectiveness of the Social Security Administration's Death Termination Process*	September 2002
A-03-02-22008	*The Social Security Administration's Employee Verification Service for Registered Employers*	September 2002
A-08-00-10047	*Audit of Enumeration At Birth Program*	September 2001
A-08-00-10061	*Replacement Social Security Cards: Opportunities to Reduce the Risk of Improper Attainment and Misuse*	September 2001
A-01-00-20043	*Old-Age, Survivors and Disability Insurance Benefits Paid to Deceased Auxiliary Beneficiaries*	June 2001
A-09-98-61011	*Improving the Usefulness of the Social Security Administration's Death Master File*	July 2000

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

Office of Audit

The Office of Audit (OA) conducts comprehensive financial and performance audits of the Social Security Administration's (SSA) programs and makes recommendations to ensure that program objectives are achieved effectively and efficiently. Financial audits, required by the Chief Financial Officers' Act of 1990, assess whether SSA's financial statements fairly present the Agency's financial position, results of operations and cash flow. Performance audits review the economy, efficiency and effectiveness of SSA's programs. OA also conducts short-term management and program evaluations focused on issues of concern to SSA, Congress and the general public. Evaluations often focus on identifying and recommending ways to prevent and minimize program fraud and inefficiency, rather than detecting problems after they occur.

Office of Executive Operations

The Office of Executive Operations (OEO) supports the Office of the Inspector General (OIG) by providing information resource management; systems security; and the coordination of budget, procurement, telecommunications, facilities and equipment, and human resources. In addition, this office is the focal point for the OIG's strategic planning function and the development and implementation of performance measures required by the *Government Performance and Results Act*. OEO is also responsible for performing internal reviews to ensure that OIG offices nationwide hold themselves to the same rigorous standards that we expect from SSA, as well as conducting investigations of OIG employees, when necessary. Finally, OEO administers OIG's public affairs, media, and interagency activities, coordinates responses to Congressional requests for information, and also communicates OIG's planned and current activities and their results to the Commissioner and Congress.

Office of Investigations

The Office of Investigations (OI) conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement of SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, physicians, interpreters, representative payees, third parties, and by SSA employees in the performance of their duties. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Counsel to the Inspector General

The Counsel to the Inspector General provides legal advice and counsel to the Inspector General on various matters, including: 1) statutes, regulations, legislation, and policy directives governing the administration of SSA's programs; 2) investigative procedures and techniques; and 3) legal implications and conclusions to be drawn from audit and investigative material produced by the OIG. The Counsel's office also administers the civil monetary penalty program.