SOCIAL SECURITY
Office of the Inspector General

October 25, 2001

The Honorable Charles E. Grassley
Ranking Minority Member
Committee on Finance
United States Senate
Washington, D.C. 20510

Dear Senator Grassley:

In response to your September 26, 2001 letter to Acting Commissioner Massanari and myself, I am pleased to provide the information you requested related to terrorist misuse of Social Security numbers (SSN).

We share the immense grief, sorrow, and rage of all American citizens at the tragic loss of life at the World Trade Center and the Pentagon on September 11, 2001—innocent men and women simply reporting for what they believed to be another day of work as well as the heroic police and firefighters, instinctively setting out to save lives, but losing their own during their gallant attempts. We are committed to providing all possible assistance in bringing to justice those responsible for these horrific crimes.

Accordingly, we have assisted the Federal Bureau of Investigation (FBI) and the Department of Justice (DoJ) in their investigative efforts. It is suspected that identity theft was a prime modus operandi of the terrorists. It has been widely reported in the media that the hijackers and their suspected accomplices committed identity theft, including at least one documented case of using a false SSN, to infiltrate the United States while planning the attacks of September 11. SSN misuse is an offense directly related to the Social Security Administration's (SSA) mission; under the Social Security Act, it is a crime to misrepresent an SSN for any purpose with an intent to deceive.

With the cooperation of the FBI, DoJ, and the Internal Revenue Service, as well as SSA, we have been able to expand our ability to share information and assist with investigative efforts directly related to the September 11, 2001 attacks. As a result, we have been able to give the FBI and other law enforcement offices valuable information leading to the arrest of suspected terrorists on charges of SSN misuse and identity theft.

Prevention of terrorist use of fake and stolen SSNs is a more difficult issue. As we discussed in our October 3, 2001 report to you, *SSN Misuse: A Challenge for the Social Security Administration*, my Office has become well acquainted with the SSN

misuse and identity theft phenomena. Through the tens of thousands of SSN misuse allegations we receive every year and the numerous cases we investigate, we have witnessed firsthand the devastating effects SSN misuse and identity theft have on innocent victims. The tragedies of last month demonstrated that SSN misuse and identity theft are "breeder" offenses with the ability to facilitate crimes beyond our imagination.

While SSA has implemented various programs to assist in the identification of SSN misuse, none are designed to uncover possible SSN misuse by noncitizens. Indeed, we can think of no program SSA could institute that would accomplish such a difficult mission. Certainly, room exists for SSA to improve its existing program and system controls to prevent the improper attainment of an SSN. However, once an individual obtains an SSN, either through proper or improper means, the Agency has little ability to control the use of that number.

Accordingly, to effectively fight crimes and combat terrorism related to SSN misuse, the Agency needs the cooperation of other Federal, State, and local law enforcement agencies as well as the criminal justice system. Additionally, Congress must make some difficult decisions before meaningful headway can be made in preventing SSN misuse by foreign nationals.

In responding to most of the questions you posed, we relied on information developed in past audits, evaluations, and investigations. The enclosed report contains our insights and conclusions regarding the following subjects.

- SSA programs and operations to identify fake SSNs and SSN cards.
- SSA programs and operations to identify stolen SSNs and SSN cards.
- SSA efforts to coordinate with other Federal agencies to identify suspected terrorists.

If you have any questions or would like to be briefed on this issue, please call me or have your staff contact Richard A. Rohde, Special Agent-in-Charge for External Affairs, at (410) 966-1722.

Sincerely,

James G. Huse, Jr.
Inspector General of Social Security

Enclosure

CONGRESSIONAL RESPONSE REPORT

Terrorist Misuse of Social Security Numbers

A-08-02-32041

OCTOBER 2001

Background

Social Security number (SSN) misuse, catalyzed by the Internet, has quickly become a serious national concern. The SSN's universality has become its own worst enemy. The power it wields—power to enable financial transactions, power to obtain personal information, power to create or commandeer identities—makes it a valuable asset and one that is subject to limitless abuse. This abuse takes many forms; SSNs are misused to commit financial thefts from companies and individuals, violate immigration laws, flee the criminal justice system by assuming a new identity, and obtain personal information to stalk an individual. Most recently, we learned that SSNs may have been misused by members of foreign terrorist organizations to infiltrate American society while planning the terrorist attacks of September 11, 2001.

One of the first steps in obtaining employment and realizing the goals of many U.S. immigrants is obtaining an SSN. Most immigrants—about 75 percent—come to the United States legally, many to join close family members. However, the Immigration and Naturalization Service (INS) estimated the undocumented immigrant population reached about 5 million in 1996, not including the 3 million who were given amnesty under the Immigration Reform and Control Act of 1986. Additionally, the INS estimates the number of undocumented immigrants continues to grow by about 275,000 individuals each year. Many undocumented immigrants do not come to the United States by crossing a border illegally. Rather, some immigrants enter legally with a student, tourist, business, or other temporary visa and become "illegal" when they stay in the United States after their visas expire.

To improperly acquire an SSN, undocumented immigrants may either apply for a "legitimate" SSN using false evidentiary documents (for example, counterfeit passports and INS documents) or create/purchase a counterfeit SSN card. Additionally, if an undocumented immigrant is not required to show an SSN card, he/she may simply invent a number. This SSN may be one the Agency has already assigned to another individual (stolen SSN) or one never assigned (fake SSN). Undocumented immigrants may obtain a false or stolen SSN to work illegally, to obtain a license, or to accomplish other tasks having nothing to do with terrorism. The Agency has mechanisms to prevent or detect some of these occurrences; however, these controls do not always work as intended and are not always used. Moreover, these mechanisms do not indicate whether the misuse is connected with possible terrorist activity.

Many of the facts and conclusions presented in this report are based on published reports and investigative results from the past 5 years. We performed report review work in Birmingham, Alabama. Other work, including summarizing the number of fake and stolen SSNs and SSN cards, was performed at the Social Security Administration (SSA) Headquarters in Baltimore, Maryland. We completed our work in October 2001.

Results of Review

On September 26, 2001, Senator Charles E. Grassley, Ranking Member, Senate Finance Committee, issued a letter to the Acting Commissioner and the Inspector General of Social Security requesting that we conduct independent assessments regarding the terrorist misuse of SSNs. Senator Grassley specifically requested that we assess three distinct elements. These elements and the Office of the Inspector General's (OIG) insights and conclusions follow.

1. DESCRIBE SSA PROGRAMS AND OPERATIONS TO IDENTIFY FAKE SS [SSN] CARDS OR SSNS.

SSA primarily focuses its resources on *preventing* individuals from improperly obtaining an SSN through its enumeration process. However, the Agency also has certain programs and operations that enable it and authorized third parties to identify false SSNs and SSN cards.[1] It is important to understand that all of these programs are designed to assist legitimate SSN-dependent activity, such as employer wage reporting, child support enforcement, and driver's license verification by States. None of these programs are designed to uncover illegal activity, such as criminal SSN misuse or identity theft, or to trigger criminal investigations. Additionally, none of these programs are designed to assist in the detection of terrorist activity. Descriptions of these programs and operations follow.

PROCEDURES FOR REVIEWING EVIDENTIARY DOCUMENTS SUBMITTED WITH SSN APPLICATIONS

When an individual applies for an original SSN, SSA requires the applicant to provide acceptable documentary evidence of *age, identity,* and *U.S. citizenship or lawful alien status.* When applying for a replacement SSN, the applicant must provide evidence of *identity* and, if applicable, *lawful alien status.* Reliable evidentiary documentation is crucial to ensuring the proper assignment of an SSN.

In examining evidence, SSA guidelines encourage employees to compare documents provided by SSN applicants with characteristics of valid documents and to be alert for alterations and erasures. SSA has equipped employees with certain tools to verify the validity of documents. Specifically, SSA provides employees copies of guides with examples of authentic documents, such as the *Administrative Confidential Memorandum* for documents issued by the INS. SSA guidelines require personnel to reference the guide and then view INS documents under a black light to ascertain whether they conform to the special identification checkpoints and fluoresce.

[1] For the purposes of this response, fake SSNs and SSN cards are those not officially assigned and issued by SSA. They include both "fake" SSNs/SSN cards and those that are stolen.

If a noncitizen has been in the United States for 30 days or more and INS has issued him/her an alien registration number, SSA policies require the use of another mechanism to verify the documents. Specifically, each SSA field office has on-line access to a data base within INS' Systematic Alien Verification for Entitlements system. Using this data base, field office personnel enter the alien registration number and compare INS information regarding the individual's status in the United States with information provided by the SSN applicant.

If, through any of these examinations, a question arises regarding the validity of the documents, SSA requires personnel to enter the application in the Modernized Enumeration System (MES) and code the evidence blocks with either an "S" for suspect documents or an "F" for known fraudulent documents. These indicators will prevent the processing of subsequent SSN applications for the applicant, whether submitted to the same or a different field office. The application will remain pending in MES until either the issuing Agency verifies the evidence and field office personnel clear the application or 120 days passes—at which time the application is deleted. If the issuing Agency reports the evidence is fraudulent, field office personnel code the application as such in MES and transfer it to the disallowed file.

SSA has implemented several other programs and procedures to address the fraudulent attainment of SSNs through its enumeration process. Descriptions of these initiatives are provided in Appendix A.

EMPLOYEE VERIFICATION SERVICE

The Employee Verification Service (EVS) provides a mechanism for employers and other third parties to match an individual's name and SSN with SSA records. Through this Service, employers can verify employee names and SSNs by (1) calling SSA's toll-free telephone number (up to 5 names), (2) submitting a list of names and SSNs to the requestor's local SSA field office (up to 50 names), or (3) submitting a paper list or magnetic media to SSA's data processing center (over 50 names). SSA will inform the employer/third party whether the information reported by the employee matches SSA's records.

Although intended to help increase the accuracy of annual wage report submissions, other authorized third parties have used EVS to ensure the validity of SSNs. In fact, SSA has been involved in SSN verification projects with several other Federal and State agencies. These include the following.

- The *SSN Feedback Pilot Project* provided error feedback messages to employers on new hire reports in collaboration with the Office of Child Support Enforcement (OCSE). OCSE maintains a national directory of all new hires, the purpose of which is to identify parents who have not complied with court-sanctioned child support agreements.[2] State agencies can impose civil monetary penalties if employers do

[2] Under the *Personal Responsibility and Work Opportunity Reconciliation Act of 1996* (Public Law No. 104-93), employers are required to submit new hire data to designated State agencies.

not comply with this requirement. The joint SSA/OCSE pilot began in July 1999, lasted just 1 year, and was limited to employers from Massachusetts and Illinois. Under the pilot, SSA verified the names/SSNs of new hires in the OCSE directory. Employers were notified within 30 days of any unverified SSNs and were asked to correct their records. However, employers were not required to resubmit corrected data. As of October 2001, SSA was still evaluating the OCSE pilot results.

- The *Basic Pilot Employment Eligibility Confirmation Program* is a joint pilot between SSA and INS. The pilot provides volunteer employers in five States query access to SSA and INS data bases to verify a new employee's name/SSN, work authorization status, and alien registration number within 3 business days after the employee is hired.[3] If the program determines an employee's name/SSN do not match SSA's records, the employer can request additional documentation from the new hire. The employer also has the option of terminating an employee who provided invalid information if the action was taken in good faith reliance on information provided through the program. The pilot began in November 1997 and will run for 4 years.

- The *Social Security On-Line Verification System (SSOLV)* assists States in the identification verification process for a driver's license. The American Association of Motor Vehicle Administrators (AAMVA) facilitates this program through its subsidiary, AAMVAnet. This on-line system allows Departments of Motor Vehicles (DMV) to submit a driver's license applicant's name, date of birth, and SSN to SSA. SSA, in turn, verifies the information against its records and instantaneously reports back to the requesting DMV whether the information matched. Currently, 12 States use the SSOLV program under a Memorandum of Understanding with SSA.[4]

EARNINGS SUSPENSE FILE

One outcome of the annual wage reporting process is the detection of invalid SSNs used to gain employment under false identities. Each year, employers must report employee earnings annually on Internal Revenue Service (IRS) *Wage and Tax Statement* (Form W-2) to SSA. W-2 wage reports that fail SSA's name/SSN match cannot be credited to workers' earnings records, but, instead, are posted to the Earnings Suspense File (ESF). The ESF contained over 227 million suspended W-2s representing more than $333 billion in suspended wages posted between Tax Years 1937 and 1999. Of the total wage reports suspended before 1999, almost 24 million wage reports (11 percent) were posted to the ESF because the employees and/or employers reported invalid SSNs (that is, numbers never issued by SSA).

Unless an employer uses one of the previously listed SSN verification programs, SSA does not become aware of invalid SSNs claimed by employees until several months

[3] The five States participating in the Basic Pilot are California, Texas, New York, Florida and Illinois.

[4] The 12 States currently using the SSOLV program include Alabama, Arizona, Maryland, Massachusetts, Mississippi, Missouri, Nebraska, Nevada, Ohio, South Carolina, South Dakota and Virginia.

after the individuals initially presented the incorrect numbers. Additionally, despite SSA efforts to contact the employees, only 8 percent of wage reports posted to the ESF are corrected through this process.[5]

In past OIG assignments, we interviewed employers, growers' associations, and SSA representatives. There was a general consensus that unauthorized noncitizens contribute significantly to SSN misuse and the growth of the ESF. In fact, several agriculture employers we interviewed acknowledged that large numbers of their workers were unauthorized noncitizens. They told us that, while they examine various types of employment eligibility documents, they know many of the documents may be fraudulent. The large number of invalid SSNs reported on wage reports and residing in the ESF seems to confirm these beliefs.

OIG INVESTIGATIONS

In Fiscal Year 2000, the OIG received 92,847 allegations of fraud, waste, or abuse. Over half of these, 46,840, were allegations of SSN misuse, and another 43,456 were allegations of program fraud, which experience has shown often includes implications of SSN misuse. Our investigations of these allegations frequently identify individuals that have obtained and/or used SSNs improperly. For example, the OIG has investigated numerous cases where individuals applied for benefits under erroneous SSNs. Additionally, we have uncovered situations where individuals counterfeit SSN cards for sale on America's streets. From time to time, we have even encountered SSA employees who sell SSNs for hundreds of dollars.

1.a. ARE THESE PROGRAMS SUFFICIENT?

Although these programs are well-intentioned, many of the following factors limit their effectiveness.

COUNTERFEIT DOCUMENTS

Given the technological advances in today's society, motivated individuals can counterfeit official documents with surprising ease and accuracy. In fact, through our audits, evaluations and investigations, we have detected numerous SSNs issued to individuals based on counterfeit evidentiary documents. For example, in 1 audit, we found that 999 of the 3,557 original SSN applications reviewed were approved based on improper evidentiary documentation.[6] We acknowledge that this is not the case with most noncitizen documents. However, our experience has shown that the error rate is significant enough to warrant increased verification of these documents.

[5] We did not determine the reliability of this figure.

[6] SSA/OIG report, *Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications*, September 2000 (A-08-98-41009).

LACK OF PARTICIPATION IN EVS

Although there were 6,000 registered users, only 211 of the 6.5 million U.S. employers used EVS in Fiscal Year 2000.[7] Employers cite many reasons for not using this tool, including its inability to verify SSNs/names instantaneously. Additionally, several employers with whom we spoke stated they were reluctant to use EVS because it was "too helpful," in that they learned many of their employees were unauthorized citizens. For example, one employer told us he hires hundreds of workers at a time, and he cannot wait weeks for a response from SSA. Another employer stated he does not want to know whether his employees are undocumented because such knowledge makes him vulnerable to fines and penalties.

Last year, SSA developed enhanced software to expand EVS to an online service—shortening the SSA response time from 2 to 4 weeks to overnight feedback. Employers have expressed an interest in this new online service. However, as we have noted in a recent audit, SSA has yet to implement this new online EVS.[8]

INABILITY TO FINE PROBLEM EMPLOYERS WHO SUBMIT WAGE REPORTS WITH INCORRECT SSNs/NAMES

SSA has no legal authority to levy fines and penalties against employers who repeatedly submit large numbers of wage reports with incorrect SSNs. As provided by law, SSA must rely on the IRS to enforce penalties for inaccurate wage reporting.[9] In a previous OIG audit, SSA senior staff stated that employers have no incentive to submit accurate annual wage reports because the IRS rarely enforces existing penalties.[10]

SSA staff believed applying penalties would have a rippling effect on employers who consistently submit wage reports for employees whose names and SSNs do not match SSA's records. Although SSA is primarily interested in penalizing the most egregious employers, IRS staff expressed concern with the application of even these penalties. IRS senior staff members believe they and SSA would have a difficult time determining whether an employer exercised appropriate diligence in obtaining the necessary information from employees. SSA representatives, however, believe the Agency could provide the IRS sufficient evidence to show an employer knew or should have known its employees' SSNs were incorrect.

---

[7] SSA does not track the number of employees that contact Teleservice Centers or local field offices to verify employee SSNs. Accordingly, we are unable to provide figures to summarize the number using these services.

[8] SSA/OIG report, *Review of Service Industry Employers with Wage Reporting Problems,* September 2001, (A-03-00-10022).

[9] Under IRS code 26 U.S.C. §6721 (a), the IRS may charge a $50 penalty each time an employer does not furnish an employee's correct SSN on a wage report.

[10] SSA/OIG report, *Obstacles to Reducing Social Security Number Misuse in the Agriculture Industry*, January 2001 (A-08-99-41004).

Despite the IRS' concerns, the two Agencies held discussions to explore the enforcement of an existing penalty provision ($50 per incorrect wage report) for employers who repeatedly submit erroneous name and/or SSN information. To implement the penalty, SSA and the IRS agreed the agencies must (1) jointly define the circumstances for applying penalties, (2) identify information needed from SSA for the IRS to support applying penalties, and (3) develop the proposed data flow and procedures to be followed.

In Calendar Year 2000, SSA provided a list of 100 of the most egregious employers to the IRS. These employers represented the employers with the largest number of name/SSN match failures in consecutive years. The IRS expressed interest in the listing but, to date, has not assessed penalties.

LACK OF INVESTIGATIVE AND PROSECUTORIAL RESOURCES FOR SSN MISUSE CASES

Another major weakness in these programs is the lack of investigative and enforcement resources needed to prosecute offenders. With limited staff and an overwhelming number of allegations, OIG's Office of Investigations (OI) prioritizes the cases it can feasibly examine. OI's first priority has traditionally been to investigate cases involving possible employee fraud. Secondly, OI attempts to examine the large volume of program cases that negatively impact Social Security trust funds. This workload constrains the ability to investigate SSN misuse connected with possible terrorist or other illegal activity not directly involving SSA programs and operations.

We acknowledge that we are unable to provide sufficient coverage to the area of SSN misuse. We cannot address the tens of thousands of SSN misuse allegations made every year. Recently, the Federal Bureau of Investigation (FBI) recognized identity fraud as the fastest growing white-collar crime in America. Unfortunately, our investigative and enforcement resources have not kept pace with this growth.

LACK OF AUTHORITY TO ASSIST TERRORIST INVESTIGATIONS THROUGH THE SHARING OF SSA INFORMATION WITH THE FBI AND THE DEPARTMENT OF JUSTICE

Section 1106 of the Social Security Act, 42 U.S.C. 1306, permits the Commissioner of SSA to restrict the disclosure of personal information in its files and SSA's regulations in this area are more restrictive than what is required under the Privacy Act. Due to the vast quantity of personal information collected by SSA, and the evil that can be done when this information falls into the wrong hands, we fully support SSA in its efforts to closely safeguard this precious information.

However, SSA's regulations prohibit the automatic disclosure of some information from SSA files to the Department of Justice (DoJ) or the FBI in connection with a terrorist

investigation, even if the request comes in writing from the Attorney General.[11] There are provisions for the Commissioner or his designee to disclose the information; however, the Commissioner must make a determination that disclosure of the information is necessary to respond to life threatening situations.[12]

In addition, SSA is prohibited from disclosing the wage and earnings information it collects to law enforcement; it is closely guarded by law under section 6103 of IRS, 26 U.S.C. § 6103.[13] Although the IRS Commissioner can authorize the disclosure by other Federal Agencies of IRS information in their possession, a determination must be made by the IRS Commissioner that there is an imminent danger of death or physical injury. 26 U.S.C. § 6103(i)(3)(B). This process has proven to be overly bureaucratic and confusing at a time when time is of the essence. There was confusion even within the U.S. Attorney's Office as to who had the authority to authorize the release of the information and the proper mechanism for obtaining such a release.

Fortunately, we have been able to get all the required authorizations to expand our ability to share information and assist with investigative efforts directly related to the September 11, 2001 attacks and have been able to assist SSA in giving the FBI and other law enforcement offices valuable information leading to arrests of suspected terrorists on charges of criminal SSN misuse and Identity Theft.

However, coordinating the necessary authorizations required an expenditure of effort and hours that delayed investigative efforts. We believe some permanent authority to assist law enforcement should be enacted. Such authority would eliminate the time and resources devoted to obtaining disclosure authority on a case-by-case basis.

We propose enactment of authority to the SSA OIG to disclose information, upon request of law enforcement, necessary to verify identity in connection with all felony investigations. The requesting law enforcement agency, knowing that a suspected felon has or has not provided genuine identity information, is better able to perform its own function. The OIG obtains important information on enumeration fraud and identity theft, and is uniquely qualified to furnish this crucial information.

We also propose enactment of authority to the SSA OIG to make broader disclosures from SSA files, including wage and earnings information, to Federal law enforcement Officers in connection with terrorist investigations. This would clarify the process and alleviate the need and precious hours spent obtaining disclosure authority on a case-by-case basis.

---

[11] SSA regulations permit disclosures to law enforcement only when a suspected criminal violation involves an SSA program "or another program with the same purpose," or "where a violent crime such as murder or kidnapping has been committed and the individual about whom the information is being sought has been indicted or convicted of that crime." 20 C.F.R. 401.155.

[12] See 20 C.F.R. § 401.195.

[13] The requirement to file W-2 reports with SSA is imposed by IRC and IRS regulations. 26 U.S.C. § 6051; 26 C.F.R. Part 31.

1.b. HOW MANY FAKE SSNS AND SSN CARDS HAS SSA IDENTIFIED IN THE LAST 5 FISCAL YEARS?

Currently, our system does not permit us to definitively distinguish between cases involving fake SSNs/SSN cards and those that are stolen. However, in the last 5 fiscal years, SSA OIG opened 5,655 cases related to SSN misuse. Each year since the creation of SSA's OIG, we have enhanced our system's capability to capture and track cases that involve SSN misuse, but we recognize that more needs to be done. In Appendix B, we provide a table that describes the various types of cases we opened over the last 5 fiscal years involving SSN misuse. This table will also serve as the response to questions 1.c., 2.b., and 2.c.

1.c. HOW MANY FAKE SSNS AND SSN CARDS WERE USED BY FOREIGN NATIONALS?

Over the last 5 fiscal years, the OIG opened 834 cases involving SSN misuse by unauthorized noncitizens. Currently our tracking system does not distinguish between cases involving fake or stolen SSNs used by foreign nationals. See Appendix B for a break out of these cases by fiscal year.

1.d. HOW CAN SSA IMPROVE ITS IDENTIFICATION OF FAKE SSNS IN THE FUTURE?

Our October 2001 report to you, *SSN Misuse: A Challenge for the Social Security Administration,* discussed certain vulnerabilities within the Agency's enumeration business process that allow the improper assignment of SSNs. SSA has considered these vulnerabilities and, to its credit, has expeditiously implemented many of the recommendations made in our reports. However, there are a number of recommendations the Agency disagreed with or has yet to implement. As a result, we believe there are still vulnerabilities within the enumeration system that allow the improper assignment and issuance of SSNs. Below is a list of recommendations we made in previous OIG reports that SSA either disagreed with or has yet to implement. We continue to support these recommendations and believe the Agency's implementation would assist in the prevention and detection of individuals attempting to improperly obtain and misuse SSNs. Accordingly, we continue to recommend that SSA:

- Obtain independent verification from the issuing Agency (for example, INS and the State Department) for all evidentiary documents submitted by noncitizens before issuing an original SSN.

- Expedite enhancements to its MES that will identify and prevent the assignment of SSNs in certain suspect circumstances.

- Establish a reasonable threshold for the number of replacement SSN cards an individual may obtain during a year and over a lifetime. SSA should then implement

controls within its system requiring management personnel to approve any SSN applications exceeding this limit.

- Provide further training to its field office employees and perform quality reviews of SSN processing.

- Seek legislative authority to provide SSA the tools to require chronic problem employers to use EVS.

- Continue pursuing with the IRS penalties on chronic problem employers. If the IRS does not enforce such penalties, SSA should seek its own sanctioning authority.

Additionally, although we have not made these recommendations in previous audit reports, we believe Congress and SSA should consider the following steps:

- Increase the number of investigative and enforcement resources provided for SSN misuse cases.

- Authorize SSA and SSA's OIG to disclose information from SSA files as requested by the DoJ and FBI in times of national emergency and in connection with terrorist investigations.

- Expand the Agency's data matching activities with other Federal, State, and local Government entities.

- Explore the use of other innovative technologies, such as Biometrics, in the enumeration process.

2. DESCRIBE SSA PROGRAMS AND OPERATIONS TO IDENTIFY STOLEN SSNS AND SSN CARDS.

In general, SSA and the OIG become aware of stolen SSNs from the applicable number holders. The victims of stolen SSNs may report the theft to SSA field office personnel or the Agency's toll-free fraud hotline.

2.a. ARE THESE PROGRAMS SUFFICIENT?

Unfortunately, in most cases, the first indication an SSN has been stolen occurs when a victim of SSN theft is denied credit or is contacted by a debt collection agency. Because very few SSN users verify the legitimacy of these numbers with SSA, the Agency typically does not learn of the misuse until it is reported by the actual number holder or another third party. Accordingly, we believe improvements should be made to programs and operations designed to identify stolen SSNs and SSN cards.

One area we believe has potential for further use in identifying stolen SSNs is data mining, which is a technique used by numerous organizations to identify suspect

activity. For example, credit card companies use data mining to document a card holder's typical spending patterns and then to identify when the individual's spending appears abnormal or suspect. With data mining, organizations can identify and stop improper activity before experiencing excessive losses. Data mining techniques to identify stolen SSNs could include the matching of SSA data bases with those maintained by States and local Governments as well as businesses and universities.

We continue to believe that Congress must pass legislation restricting future use of SSNs. Unfortunately, we realize that it is impossible to turn the clock back to a time when SSNs were used solely for tracking wages and making benefit payments. The SSN has become our de facto national identifier. Certainly, if fewer entities relied on the SSN as an identifier, the motivation for stealing SSNs would wane. However, given recent events, we realize that (1) a complete restriction on SSN use is impractical and (2) stopping SSN misuse, through whatever technology and means are available, is paramount. Accordingly, we encourage Congress to take a hard look at the appropriate uses for SSNs, restrict use to those purposes, and allow the use of advance technology to track down and prevent SSN misuse.

2.b. HOW MANY STOLEN SSNS AND SSN CARDS HAS SSA IDENTIFIED IN THE LAST 5 FISCAL YEARS?

See Appendix B for the total number of SSN misuse cases opened over the last 5 fiscal years.

2.c. HOW MANY STOLEN SSNS AND SSN CARDS WERE USED BY FOREIGN NATIONALS?

Over the last 5 fiscal years, the OIG opened 834 cases involving SSN misuse by unauthorized noncitizens. Currently, our tracking system does not distinguish between cases involving fake or stolen SSNs used by foreign nationals. See Appendix B for a break out of these cases by fiscal year.

2.d. HOW CAN SSA IMPROVE ITS IDENTIFICATION OF STOLEN SSNS IN THE FUTURE?

We believe the Agency and Congress should focus on *preventing* the theft of SSNs. Specifically, we believe legislation is needed to limit the use of SSNs. In his May 2001 testimony before the House Committee on Ways and Means, Subcommittee on Social Security, the Inspector General stated the following.

> *We need legislation that limits the use of the SSN to those purposes that benefit the holder of the SSN, . . . legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. I am sensitive to the costs that would be incurred in both the public and the private sectors in implementing the changes that such legislation would require, and I do not suggest that any of us are facing an easy task. Rather it is a necessary task. The appropriate*

agencies, in cooperation with governmental authorities and business leaders, must reach an understanding as to the need to limit the use of the SSN and regulations would have to be promulgated reflecting such uses and providing for enforcement mechanisms. In addition, the legislation would need to outlaw the sale of SSNs over the Internet and through other means. With certain legislated exceptions, no private citizen, no business interest, and no ministerial government agency should be able to sell, display, purchase, or obtain any individual's SSN, nor should they be able to use any individual's SSN to obtain other personal information about the individual.

As previously discussed, we also encourage Congress and SSA to consider advanced technologies, such as Biometrics and data mining, to improve the integrity of the SSN and provide early detection of stolen and/or misused SSNs and SSN cards.

3. Describe SSA Efforts to Coordinate with Other Federal Agencies to Identify Suspected Terrorists. Specify Any Coordinate Efforts and Sharing of Resources with the Immigration and Naturalization Service (INS). Also, Describe How SSA Can Improve Its Coordinative Efforts with Other Federal Agencies and Particularly with INS.

Our efforts to coordinate with other Federal agencies to identify suspected terrorists involved in the September 11, 2001 attacks on Washington, D.C., and New York City are described in the following sections.

IMMEDIATE RESPONSE

The SSA OIG became immediately involved and remained involved in the terrorist investigation because of the nature of our jurisdiction with respect to the integrity and use of SSNs and the records SSA maintains as a consequence of that activity. Descriptions of our immediate response measures follow.

September 11

- SSA OIG special agents arrived at the World Trade Center immediately assisting in rescue efforts.

September 12

- In New York City, we detailed 10 OIG employees (1 supervisor and 9 agents) to the FBI command center to process information and investigate leads. We also detailed six New Jersey employees (a supervisor and five agents) to the FBI's Newark command center.

- Two Boston OIG agents responded to the Westin Hotel in Boston where the FBI executed search warrants and detained a number of suspected accomplices. The agents provided information confirming one suspect was using an assumed name.

PROVIDING INFORMATION

As the investigation progressed, it became obvious that extensive data would be needed from SSA's records regarding the identities of the terrorists and potential accomplices. The FBI, in a memorandum from its Director, formally requested SSA OIG's participation in the "PENTTBOMB" investigation. We immediately assigned personnel to the FBI's Strategic Information and Operations Center; the National Infrastructure Protection Center in Washington, D.C.; and the Baltimore FBI Office, which was designated as the national clearing house for FBI requests for SSN information. To further the investigation's efforts, OIG supervisors petitioned to and received from the Commissioner of SSA the authority for the OIG to disclose SSA program information as necessary to respond to life threatening situations. In addition, at the OIG's request, SSA sought authorization from the Commissioner of IRS to disclose wage and earnings information contained in SSA records, citing the "Imminent Danger" clause of the IRS code. The IRS authorized SSA to made the disclosures for a period of 30 days from the date of the authorization and provided that the authorization could be extended if the imminent danger was still in existence after that time.

Record Searches

The weekend following the attack, our agents reported to work in seven States to conduct record searches for information on suspected terrorists and their movements nationwide. This information contributed to the issuance of many arrest and search warrants. Our computer staff has also queried more than 1 billion SSA records to provide information identifying subjects and potential cell locations.

Cooperation with Other Agencies

SSA has supported the massive data collection effort by dedicating five mainframe servers to process and retain these queries. SSA has also cooperated by authorizing full disclosure of SSA information to law enforcement officers. To provide complete information, we negotiated an agreement with SSA and the IRS that allows disclosure of wage and earnings information maintained by SSA to the FBI. Many investigative leads and warrants have been generated as a result of this information. In addition to SSA and the IRS, the OIG OI met with the INS to share the information we currently have available. We also agreed to continue exchanging information to further the investigation. Verification of documents via INS is an integral part of validating information of immigrants who applied for or obtained SSNs and thus an important part of any related investigation.

Continued Commitment

As INS Detainers and Material Witness warrants expire, many of these suspects are being charged with criminal SSN misuse and identity theft. Besides bringing these serious offenses to justice, these actions ensure that the suspected terrorists remain in the judicial process while the terrorist investigation is continuing. To this end and to further the investigation, at any given time, many OIG employees are working exclusively on investigative matters relating to the FBI's PENTTBOMB investigation. There are also many additional agents responding to false SSN applications that are being reported by SSA employees throughout the country.

We would also like to note that, in addition to supporting the investigation, SSA OIG agents assisted SSA in establishing processing centers to work with the families of the victims of the attack to expeditiously process benefits available to them through SSA programs. We realize that, for many of the victims, their only direct contact with the Government in the aftermath of the attacks may be with the SSA when they apply for benefits. We are sensitive to our obligation to support SSA in its efforts to do its best work at this time, while leaving the actual work of the SSA to the SSA Officers and hard-working employees, in accordance with the Inspector General Act.

HOW SSA CAN IMPROVE ITS COORDINATIVE EFFORTS WITH OTHER FEDERAL AGENCIES AND PARTICULARLY WITH INS

With regard to identifying terrorists, we believe we are doing everything possible to coordinate with other Federal agencies. While we acknowledge that no system is perfect, we know of no systemic improvements that should be implemented. In the future, Congress may wish to adopt permanent authority for SSA and the SSA OIG to assist with terrorist investigations as we are doing now. Such permanent authority would decrease the precious time associated with the need to obtain enhanced disclosure authority on a case-by-case basis.

Conclusion

In recent years, we have seen the enactment of *The Identity Theft and Assumption Deterrence Act of 1998* and the *Internet False Identification Prevention Act of 2000*. The former is the first legislative response to the growing wave of identity thefts and imposes criminal sanctions for those who create false identities or misappropriate someone else's. The latter closed a loophole left by the first, enabling law enforcement agencies to pursue those who could previously sell counterfeit SSN cards legally, by maintaining the fiction that such cards are "novelties," rather than counterfeit documents. Both pieces of legislation are helpful, but both treat the identity theft disease in its latest stages, rather than at its onset. In most cases, identity theft begins with the misuse of an SSN, and, while the ability to punish identity theft is important, the ability to *prevent* it is even more critical.

How do we do this? First and foremost, the time has come to control and strengthen the use of the SSN. We as a Government created the SSN, and we as a Government must control it. We must make the difficult determinations as to those uses that are appropriate and necessary, and those that are merely convenient. The SSN is a unique identifier, and its quotidian use as identification by schools, hospitals, and other institutions is understandable—but dangerous without implementing strong integrity controls and enforcement.

Reliance on SSNs as identifiers is increasing the motivation to steal, create, or improperly obtain these numbers. Accordingly, we urge Congress to consider enacting legislation that limits use of the SSN to specific purposes and provides for stronger controls over its issuance and maintenance. Additionally, we continue to support previous recommendations we have made to SSA regarding verification of immigration documents presented with SSN applications. We recommend the adoption of limited permanent disclosure authority that will permit SSA and SSA OIG to assist terrorist investigations. Finally, we recommend the Agency and Congress consider the use of advanced technologies, such as Biometrics and data mining techniques, to enhance the integrity of the SSN.

Appendices

Other Social Security Administration Actions to Address the Fraudulent Attainment of Social Security Numbers

In its Annual Strategic Plan, the Social Security Administration (SSA) included the goal of making "SSA program management the best in the business, with **Zero Tolerance for Fraud and Abuse**" (emphasis added). In line with this policy, SSA implemented several initiatives designed to address the fraudulent attainment of Social Security numbers (SSN). Some of the Agency's current and planned initiatives include the following.

- *Age 18 and over Procedures:* SSA implemented unique procedures for processing original SSN applications submitted by individuals age 18 years or older. These procedures ensure applicants do not already have an SSN and are not attempting to inappropriately secure a new SSN.

- *Collection of Enumeration Data by the Immigration and Naturalization Service (INS) and the Department of State:* SSA, INS and the Department of State are working on agreements that will enable INS and the Department of State to collect enumeration data from aliens entering the United States. Although SSA will still process the SSN applications, the agencies believe this initiative will significantly reduce the possibility of SSA accepting counterfeit documentation and will eliminate duplicate contacts that aliens now must make to obtain SSNs.

- *Comprehensive Integrity Review Program:* In March 1999, SSA began using a new version of one of its integrity software programs. Among other features, the automated system identifies instances in which five or more SSN cards are sent to the same address within a 5-week period. This system generates alerts to the SSA field offices for preliminary investigation.

- *SSA Access to State Records On-line:* SSA is working with States through the National Association of Public Health Statistics and Information Systems to allow field offices on-line access to State vital records data. Implementation of this initiative is contingent on obtaining agreements with all of the States and jurisdictions first for accessing in-State data and then separate agreements so data can be shared across State lines. However, once implemented, field offices will be able to verify all U.S. birth certificates presented in support of SSN applications.

- *Access to INS' Nonimmigrant Index System:* SSA and INS are working to provide all field offices on-line access to INS' Nonimmigrant Index System. This system will allow SSA personnel to verify documents submitted by nonimmigrants. Currently, SSA can only verify documents submitted by immigrants with alien registration numbers through the Systematic Alien Verification for Entitlements program.

- *More Preventive Controls Within the Modernized Enumeration System:* In response to a previous Office of the Inspector General report, SSA established a workgroup tasked with identifying enhancements that could be made in the Modernized Enumeration System to address two fraud-prone situations: (1) when parents allege having an improbably large number of children and (2) when SSA sends a large number of SSN cards to the same address. The workgroup is working to finalize and implement its recommendations.[1]

[1] SSA/OIG report *Using Social Security Numbers to Commit Fraud*, May 1999 (A-08-99-42002).

Social Security Number Misuse Cases Opened by OIG in Fiscal Years 1997 Through 2001

Nature of Allegations	FY 1997 Cases Opened	FY 1998 Cases Opened	FY 1999 Cases Opened	FY 2000 Cases Opened	FY 2001 Cases Opened	TOTALS
SSN Misuse/ General	1,144	928	454	398	234	3,158
SSN Misuse/ Illegal Alien	23	23	186	354	248	834
False Statement to Obtain SSN	274	151	117	209	160	911
Selling Counterfeit SSN Cards	46	26	21	39	54	186
Selling Legitimate SSN Cards	21	8	14	19	28	90
Use or Possession of Counterfeit SSN Card	48	51	26	37	33	195
False Identity	16	26	34	88	117	281
TOTALS	1,572	1,213	852	1,144	874	5,655

SSN = Social Security Number
FY = Fiscal Year

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kim Byrd, Acting Director, Operations Audit Division (205) 801-1605

Acknowledgments

In addition to those named above:

Kathy Youngblood, Senior Auditor

Steven Barry, Program Manager

Tim DeHoff, Investigator

Judy Ringle, Attorney