
**OFFICE OF
THE INSPECTOR GENERAL**

SOCIAL SECURITY ADMINISTRATION

**SOCIAL SECURITY NUMBER
INTEGRITY: AN IMPORTANT LINK
IN HOMELAND SECURITY**

May 2002 A-08-02-22077

**MANAGEMENT
ADVISORY REPORT**



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.



SOCIAL SECURITY

MEMORANDUM

Date: May 9, 2002

To: The Commissioner

From: Inspector General

Subject: Social Security Number Integrity: An Important Link in Homeland Security
(A-08-02-22077)

OBJECTIVE

The objective of this Management Advisory Report is to provide information regarding (1) how Social Security number (SSN) integrity has become a critical element in the protection of our homeland, (2) what the Social Security Administration (SSA) and SSA's Office of the Inspector General (OIG) have done to ensure the SSN's integrity, and (3) what tasks remain in this important effort.

BACKGROUND

As the Office of Homeland Security stated in its report, *Securing the Homeland, Strengthening the Nation*, "The Government of the United States has no more important mission than fighting terrorism overseas and securing the homeland from future terrorist attacks." Federal agencies, including SSA, have embraced this challenge—one of monumental scale and complexity. We believe strengthening SSN integrity is one way in which SSA can make an important contribution to this national goal.

In the past, OIG has issued numerous reports addressing SSN integrity (Appendix A). These reports included recommendations that addressed vulnerabilities in several SSA processes including SSN assignment and issuance, employer wage reporting, and death master file reporting and issuance. SSA elected to implement many of these recommendations. Additionally, after the events of September 11, 2001, SSA revisited its position on many prior OIG recommendations that it had either not yet implemented or disagreed with. In several cases, SSA decided to escalate the implementation of some recommendations, while it reversed its position on others.

SCOPE AND METHODOLOGY

In preparing this report, we obtained and reviewed information from various sources, including the Office of Homeland Security's web site, previous OIG reports, statistics and case summaries from our Office of Investigations and Fraud Hotline, and preliminary drafts of certain legislation. Although we did not perform an audit of a specific SSA entity, most of the information contained herein relates to responsibilities of the Office of Program Benefits under the Deputy Commissioner for Disability and Income Security Programs. We performed this work in March 2002 in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.

RESULTS OF REVIEW

We have long been aware that failure to protect the integrity of the SSN has enormous financial consequences for the Government, the people, and the business community. We now know that shortcomings in the SSN issuance process can have far graver consequences than previously imagined. The difficult lessons of September 11, 2001 have taught us that SSA can no longer afford to operate from a "business as usual" perspective. Whatever the cost, whatever the sacrifice, we must protect the number that has become our national identifier; the number that is the key to social, legal, and financial assimilation in this country.

We recognize SSA alone cannot resolve the monumental issues surrounding homeland security. Efforts to make our Nation safer will involve new or expanded initiatives by almost every segment of our population, including State and local governments, private industry, non-governmental organizations, and citizens. However, we also recognize that, in endeavoring to protect our homeland, no Government system or policy should be ignored. As such, SSA, as a Federal agency and public servant, must resolve to review its systems and processes for opportunities to prevent the possibility that anyone might commit or camouflage criminal activities against the United States. We believe SSN integrity is a link in our homeland security goal that must be strengthened.

HOW DOES SSN INTEGRITY IMPACT HOMELAND SECURITY?

How can we assist the Administration's efforts to investigate the initial attacks and prevent future attacks?

In the weeks following September 11, concerned citizens across the Nation asked many questions about the terrorists. For example, how were these individuals able to assimilate into our society? What documentation allowed them to do so, and how did they obtain it? Are there more terrorists hiding in the United States, and, if so, how can law enforcement officials locate them? Who are their supporters in the United States? Most importantly, many asked "how can we assist in efforts to investigate the attacks and prevent future attacks?"

For SSA's OIG, the answer to many of these questions revolved around one item—the SSN. A unique set of nine numbers assigned to almost everyone in the United States. In fact, today, approximately 300 million people have an SSN. The SSN is critical to SSA's implementation of its programs and operations. While this was originally the SSN's only intended use, the SSN quickly became our de facto national identifier, used as a key means of identification in both the public and private sectors.

As use of the SSN has grown, so has its misuse. Because the SSN is so heavily relied upon as an identifier, it is a valuable commodity for criminals. It can be obtained illegally in many ways: presenting false documentation to SSA; stealing another person's SSN; purchasing an SSN on the black market; using the SSN of a deceased individual; and creating a nine-digit number out of thin air. As we have learned through the terrorist investigations, even a legally obtained SSN can be used to facilitate an unlawful act.

In Fiscal Year 2001, OIG's Fraud Hotline received over 115,000 allegations of fraud. Of this total, over 55 percent were allegations of SSN misuse. Examples of this type of fraud include use of an improperly obtained SSN to obtain a driver's license or a credit card, open a bank account, or secure a loan. The remaining allegations were of program or employee fraud, receipt of Social Security benefits, or other fraud having a direct effect on the Social Security Trust Fund. Experience has shown that these cases often also include implications of SSN misuse.

Given the magnitude of such allegations and competing priorities, OIG is regrettably unable to investigate a large percentage of the possible criminal violations involving SSN misuse. Nevertheless, in response to the September 11 attacks, we have committed extensive resources to investigating cases in which SSNs may have been used to facilitate or camouflage terrorist crimes. The following examples summarize a few of the many cases we pursued involving SSN misuse and possible terrorist activity or connections. These cases also illustrate SSA's vulnerability to counterfeit evidentiary documents that individuals sometimes use to inappropriately obtain an SSN.

- ✓ On December 6, 2001, a Federal Grand Jury in Phoenix, Arizona, returned a 41-count indictment against an individual for, among other crimes, 2 counts of *Furnishing False Information as an Identity to Obtain an SSN* and 25 counts of *Using an SSN Assigned to Someone Else*. The Investigation revealed that the individual, a licensed commercial pilot, obtained an initial SSN in July 1992 in Mesa, Arizona. In August 1999, the individual used a counterfeit Somali passport in another name to obtain an additional SSN.

The indictment stated the individual interchanged the names and SSN's on a variety of official documents, including Federal Aviation Administration documents. He also obtained driver's licenses in both names and used both identities on a variety of loan and credit card applications, leases and more.

- ✓ Based on a referral from an SSA field office employee, SSA's OIG and other law enforcement agencies arrested an individual for possessing counterfeit documents, violating the Immigration and Nationality Act, and filing a fraudulent SSN application. The individual had a Pakistani passport that contained a counterfeit non-immigrant U.S. visa and a counterfeit I-94, *Arrival/Departure Record*. He also had a genuine SSN card; a counterfeit, blank SSN card; a counterfeit Alien Registration card; and numerous credit cards.

The individual obtained the genuine SSN card by submitting an application to SSA with the counterfeit non-immigrant visa as proof of his immigration status. The suspect stated he filed for an SSN twice. The first time he filed, he was denied, but he received an SSN on his second try at a different SSA field office. The suspect purported to have paid \$1,200 for the counterfeit U.S. visa and SSN card.

In addition, our Office of Audit (OA) is conducting an audit in which we are reviewing SSA's procedures for verifying documents submitted with SSN applications. Although we plan to issue the final report in the Summer of 2002, preliminary results indicate that approximately 8 percent (over 100,000) of the 1.2 million original SSNs assigned to non-citizens in Calendar Year 2000 may have been based on invalid immigration documents. We believe results and examples like those cited above illustrate the necessity to verify all evidentiary documents submitted with SSN applications. We recognize SSA is moving toward this goal; however, we are concerned that delays in implementation could result in thousands more improperly assigned SSNs. Accordingly, we urge the Agency to establish a firm time frame by which it will commit to independently verifying all immigration documents before assigning an SSN.

WHAT STEPS HAVE SSA AND OIG TAKEN TO ADDRESS THIS CRITICAL ISSUE?

Both SSA and OIG promptly accepted the challenge of addressing the Agency's role in homeland security. Recognizing the SSN's importance in non-citizens' assimilation in U.S. society, SSA established an Enumeration Task Force to examine and establish policy that would strengthen the Agency's procedures. As a member of this Task Force, OIG has shared many insights and ideas with the Agency, which we believe will help increase the integrity of the enumeration process. Additionally, since moments after the initial terrorist attacks, OIG has been fully engaged in investigating these crimes. We assisted in search, rescue and recovery efforts, and we devoted extensive resources to developing information regarding possible co-conspirators in the attacks. As evidenced by our actions, SSA and OIG are committed to bringing to justice individuals who participated in these terrible acts and improving procedures for ensuring SSN integrity, thereby strengthening our link in the homeland security chain.

ENUMERATION TASK FORCE

The Enumeration Task Force is re-examining the entire enumeration process, including previous OIG recommendations, to identify ways SSA can strengthen its enumeration policies and procedures. On November 1, 2001, SSA's then-Acting Commissioner issued a memorandum to SSA executive staff announcing seven reforms the

Enumeration Task Force recommended and the Agency would implement to address enumeration-related vulnerabilities. In that memorandum, the Acting Commissioner committed that SSA would institute these reforms by February 2002. Additionally, the Enumeration Task Force added another planned initiative to the list after the November 2001 memorandum, bringing the total short-term projects to eight. SSA has implemented several of these initiatives, while others have been delayed. A chart containing the status of each initiative is included as Appendix B. These initiatives are as follows.

1. Provide refresher training on enumeration policy and procedures, with emphasis on enumerating non-citizens, for all involved staff.
2. Convene a joint task force between SSA, the Immigration and Naturalization Service (INS), the Department of State (DoS), and the Office of Refugee Resettlement to resolve issues involving enumeration of non-citizens, including working out procedures for verifying INS documents before SSN issuance.
3. Eliminate driver's licenses as a reason for a non-work number.
4. Provide an alternative to giving out a Numident printout for SSN verification.
5. Lower the age tolerance from age 18 to age 12 for mandatory interview procedures, including verification of birth records before enumeration for all applicants age 1 and over for original SSNs and require evidence of identity for all children, regardless of age.
6. Determine the feasibility of photocopying (or scanning) all documentary evidence submitted with SSN applications.
7. Change the Modernized Enumeration System to provide an electronic audit trail, regardless of the mode used to process SSN applications.
8. Implement the SSN Verification System.

OIG INITIATIVES

OIG has taken the challenge of addressing homeland security and the SSN's role in this endeavor seriously. We are committed to providing whatever assistance we can in bringing to justice those who committed the unfathomable terrorist acts against our Nation. Additionally, we will provide whatever knowledge and resources we have to affect significant changes in Federal programs so that not one more terrorist can use our own systems and processes to facilitate such crimes. As evidenced by the myriad efforts OIG has already taken, our resolve is deep.

Investigative Efforts

OIG special agents, computer specialists, and attorneys have long worked closely with Federal, State and local law enforcement officials to investigate and prosecute SSN misuse. Since September 11, we have further increased our efforts in this area, working aggressively to support the Administration's efforts to investigate the attacks and prevent future incidents. Examples of our efforts follow.

- ✓ Within minutes of the attack on the World Trade Center, the Special Agent-in-Charge for OIG New York Field Division contacted the Federal Bureau of Investigation (FBI), offering the services of all the special agents under his command. In the days following the attacks, several of these special agents assisted in search, rescue and recovery efforts at Ground Zero.
- ✓ Nationally, OIG has been an active participant in the FBI's Joint Terrorism Task Force. We have provided round-the-clock support to the national criminal investigation of the terrorist attacks. Our special agents, computer specialists, and attorneys have helped identify, detain, indict, and convict individuals who may have a relationship with terrorist activities.
- ✓ OIG quickly assigned its agents in the New York/New Jersey area to the FBI investigation. Additionally, OIG had representatives assigned to the FBI's Strategic Information and Operations Center and to the National Infrastructure Protection Center. The OIG's Electronic Crimes Team assisted the FBI, while our computer specialists wrote programs to more specifically query SSA's data bases for FBI-requested information. Additionally, OIG agents fielded SSN information requests on suspects and witnesses, each of which was routed through the FBI's Baltimore office to our Headquarters. Many SSA OIG investigators are working full-time on the terrorism investigation and responding to allegations of SSN misuse.
- ✓ "Operation Safe Travel" began in September 2001 when SSA OIG agents developed information that individuals working at the Salt Lake City International Airport were misusing SSN's for security badge applications and I-9's, (*Employment Eligibility Verification*). Under the direction of the U.S. Department of Justice (DoJ), investigators subpoenaed records for all 9,000 airport employees with security badges to identify instances of SSN misuse. They identified 61 individuals with the highest-level security badges and 125 individuals with lower level badges who misused SSN's. A Federal grand jury indicted 69 individuals for Social Security and INS violations. Sixty-one of the 69 individuals arrested had an SSN misuse charge by the U.S. Attorney. On December 11, 2001, SSA's OIG agents and other members of the Operation Safe Travel Task Force arrested 50 individuals. To date, more than 20 have been sentenced after pleading guilty to violations cited in the indictments. Many are now involved in deportation proceedings. There were other similar airport operations after the Salt Lake City Operation, and more are underway. In conjunction with DoJ, we are looking at other critical infrastructure facility sites.

Audit Efforts

Our OA produced in-depth responses to two congressional inquiries assessing SSA's policies and procedures for issuing original and replacement Social Security (SS) cards. In early October 2001, we assessed SSA's business processes for issuing and protecting SSNs. This assessment addressed evidence presented with SSN applications; computerized controls; SSA's accounting for SS cards; additional training for SSA employees; public awareness on the proper use and dissemination of the SSN; and SSA's coordination efforts with other Federal agencies.

Later in October, we assessed SSA's programs and operations to identify counterfeit and stolen SS cards and described SSA's coordination efforts with other Federal agencies to identify suspected terrorists. Additionally, in October, we provided our views to SSA's Enumeration Task Force on techniques to improve SSN verification and decrease incidents of identity theft with new categories of SSNs, suggestions on photograph identifications, and additional automated controls.

Our OA is conducting a follow-up review of SSA's procedures for verifying evidentiary documents presented by non-citizens in applying for original SSNs. We will evaluate SSA's progress in implementing prior recommendations and also quantify the extent to which SSA is detecting false documents presented by foreign-born individuals.

WHAT TASKS REMAIN TO ENSURE SSN INTEGRITY IN A POST-SEPTEMBER 11TH ENVIRONMENT?

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 Federal legislative response to the growing wave of identity thefts and imposes criminal sanctions for those who create false identities or misappropriate someone else's. It is also the first piece of legislation that recognized the SSN as a means of identification. The latter closed a loophole left by the first, enabling law enforcement agencies to pursue those who could previously sell counterfeit SS cards legally, by maintaining the fiction that such cards are "novelties," rather than counterfeit documents. Both pieces of legislation are helpful but mainly treat the identity theft disease in its later 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? Our audit and investigative work has shown that there are three stages at which protections for the SSN must be put in place: upon issuance, during the life of the number holder, and upon that individual's death.

Assignment/Issuance of an SSN

In Fiscal Year 2001, SSA issued over 18.4 million original and replacement SS cards. Approximately 1.5 million of the original SSNs were issued to non-citizens. When SSA assigns an SSN or issues an SS card, it is critical that SSA independently verify the authenticity of the birth records, immigration records, and other identification documents the applicant presented.

In several previous audit reports, OIG recommended independent verification of birth and immigration records submitted to support an SSN application. Additionally, we recommended full and expedited implementation of a joint Enumeration at Entry program to issue SSNs to non-citizens upon their entry into the United States with the INS and DoS. However, before September 11, the Agency disagreed with our recommendation to independently verify birth and immigration records. The Agency stated that delaying the receipt of SSNs for thousands of non-citizens, most of whom were legitimately entitled to a number, was not acceptable. Rather, they preferred to work with the INS on improving existing systems until the Enumeration at Entry program could be implemented. Unfortunately, until September 11, SSA had little success encouraging the INS to move quickly on either of these planned initiatives. SSA representatives have reported that negotiations with INS are proceeding more smoothly and at a faster pace.

SSA's Enumeration Task Force recommended that the Agency seek independent verification of all non-citizen documents before assigning an SSN. Additionally, the Agency is planning to implement a process requiring verification of all U.S. birth certificates for anyone applying for an SSN after the age of 1. We believe implementation of these actions will have an immediate positive impact on the assignment of SSNs based on fraudulent documents. Both recommendations were also included in House Bill 2036, *The Social Security Number Privacy and Identity Theft Prevention Act of 2001*. This legislation would *require* SSA to verify birth records and provide a status report, with the Attorney General, on the joint initiative to enumerate non-citizens at entry.

Unfortunately, full implementation of the initiative to verify immigration documents has been delayed, perhaps for 6 months or more. SSA is waiting for the INS to incorporate information on certain immigrants with work authorization in its data base. Additionally, another delay will be necessary while SSA and the INS work out the details for obtaining access to the INS' data base on non-immigrants or those who may have temporary authorization to work in the United States. As a result, for at least several more months, SSA will continue to issue SSNs to non-citizens without obtaining independent verification of evidentiary documents from the issuing agency.

This continued practice concerns us greatly. We understand the agencies need sufficient time and planning to effectively adopt the Enumeration at Entry program. However, we strongly believe the Agency should immediately begin verifying non-citizen documents before issuing SSNs, regardless of the time delay required for the individual

to obtain an SSN. While SSA should strive for timely customer service, this desire must be balanced against enumeration integrity and the security of our Nation's borders. To emphasize the importance of the implementation of the Enumeration at Entry program, we recently issued correspondence to the Inspectors General for DoJ and DoS asking that they advise us of the feasibility of INS and DoS meeting the proposed due dates for systems changes needed to support the program.

Protection During the Life of the Number Holder

Once SSA issues an SSN and it becomes an integral part of the number holder's life, it becomes difficult to give the SSN the degree of privacy it requires. Businesses and Government agencies nationwide rely on the SSN as a convenient means of record keeping. By doing so, these entities collect, store, and, sometimes, share a lifetime of personal information associated with the number. With this information, a criminal can commit financial fraud, and, in some cases, camouflage other crimes. The challenge for SSA and the Congress is to find a balance between ensuring the SSN's privacy and ensuring that businesses and Federal and State agencies are not unduly limited in the process. Despite this challenge, there are important steps we can take.

- ✓ ***Limit the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.***

We recognize it is virtually impossible to turn back the clock and limit the use of the SSN to Federal programs. We have, therefore, focused our efforts on limiting the public availability of SSN information. We have worked with Federal, State, and local agencies; SSA; the Congress; and the public to strengthen controls over the SSN and prosecute those who misuse it. Several of our recommendations are contained in pending legislation, including provisions in Senate Bill 848, the *Social Security Number Misuse Prevention Act of 2001*; Senate Bill 1055, the *Privacy Act of 2001*; and House Bill 2036, the *Social Security Number Privacy and Identity Theft Prevention Act of 2001*.

- ✓ ***Prohibit the sale of SSNs, prohibit their display on public records, and limit their use to valid transactions.***

Recent and proposed legislation addresses important elements in protecting one's SSN. We support the pending legislation and encourage Congress to expedite such measures.

- ✓ ***Enact strong enforcement mechanisms and stiff penalties to further discourage SSN misuse.***

OIG special agents and attorneys have long worked closely with Federal, State and local law enforcement officials to investigate and prosecute SSN misuse. Since September 11, we have further increased our efforts in this area, working aggressively to support the Administration's efforts to investigate the attacks and

prevent future incidents. However, we have been limited in our ability to respond to these concerns as a consequence of balancing priority matters with existing resources. We believe more resources should be directed to investigating and prosecuting such crimes.

Protection of the SSN After the Number Holder's Death

Finally, we must do more to protect the SSN after the number holder's death. SSA receives death information from a variety of sources and compiles a Death Master File, which is updated monthly, transmitted to various Federal agencies, offered for sale to the public, and available for access over the Internet. There is no question this information must be accurate. However, we also believe the practice of offering this information to the general public needs serious consideration.

CONCLUSION

SSA and OIG promptly responded to the challenge of ensuring SSN integrity as a part of homeland security efforts. We recognize that "business as usual" is no longer permissible and have committed significant resources and energy in developing improved procedures in our enumeration business practice. Despite SSA's commitment to this endeavor, more needs to be done to ensure the SSN's link to homeland security is strong and durable. We believe that the current efforts of the Executive Branch and the Congress to work together to address these concerns will continue.

AGENCY COMMENTS

As we made no recommendations in the report, SSA elected not to provide a formal response. Rather, the Agency provided minor technical comments, which we have incorporated where appropriate.



James G. Huse, Jr.

Appendices

Appendix A – Prior Office of the Inspector General Audit Reports

Appendix B – Status of Enumeration Task Force Recommendations

Appendix C – Acronyms

Appendix D – OIG Contacts and Staff Acknowledgment

PRIOR OFFICE OF THE INSPECTOR GENERAL AUDIT REPORTS

Social Security Administration Office of the Inspector General Reports Related to Social Security Number Integrity	
<i>Name and Common Identification Number</i>	<i>Date Report Issued</i>
<i>Canada's Experience in Charging a User Fee for Social Insurance Number Cards (A-06-97-62003)</i>	May 1997
<i>Management Advisory Report: Activity Related to the Suspense File (A-03-96-31001 and A-03-96-31002)</i>	September 1997
<i>Follow-Up of the Internal Controls over the Modernized Enumeration System (A-04-96-44001)</i>	March 1998
<i>Payment of Benefits to Individuals Who Do Not Have Their Own Social Security Number (A-04-96-42000)</i>	March 1998
<i>Performance Measure Audit: Timely Issuance of Social Security Number Cards (A-02-97-93003)</i>	April 1998
<i>Assessment of the Social Security Administration's Processing of Requests for Social Security Numbers in Emergency Situations (Limited Distribution) (A-08-97-44001)</i>	June 1998
<i>Management Advisory Report: Using Social Security Numbers to Commit Fraud (A-08-99-42002)</i>	May 1999
<i>Management Advisory Report: Analysis of Social Security Number Misuse Allegations Made to the Social Security Administration's Fraud Hotline (A-15-99-92019)</i>	August 1999
<i>Patterns of Reporting Errors and Irregularities by 100 Employers with the Most Suspended Wage Items (A-03-98-31009)</i>	September 1999
<i>Review of Controls Over Nonwork Social Security Numbers (A-08-97-41002)</i>	September 1999

<i>The Social Security Administration is Pursuing Matching Agreements with New York and Other States Using Biometric Technologies (A-08-98-41007)</i>	January 2000
<i>Performance Measure Review: Reliability of the Data Used to Measure Social Security Number Request Processing (A-02-99-01009)</i>	March 2000
<i>Improving the Usefulness of the Social Security Administration's Death Master File (A-09-98-61011)</i>	July 2000
<i>Effectiveness of Internal Controls in the Modernized Enumeration System (A-08-97-41003)</i>	September 2000
<i>Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications (A-08-98-41009)</i>	September 2000
<i>Obstacles to Reducing Social Security Number Misuse in the Agriculture Industry (A-08-99-41004)</i>	January 2001
<i>Force Processing of Magnetic Media Wage Reports with Validation Problems (A-03-99-31001)</i>	May 2001
<i>Management Advisory Report: Review of Service Industry Employer with Wage Reporting Problems (A-03-00-10022)</i>	September 2001
<i>Audit of the Enumeration at Birth Program (A-08-00-10047)</i>	September 2001
<i>Replacement Social Security Number Cards: Opportunities to Reduce the Risk of Improper Attainment and Misuse (A-08-00-10061)</i>	September 2001
<i>Congressional Response Report: SSN Misuse – A Challenge for the Social Security Administration (A-08-02-22030)</i>	October 2001
<i>Congressional Response Report: Terrorist Misuse of Social Security Numbers (A-08-02-32041)</i>	October 2001
<i>Disclosure of Personal Beneficiary Information to the Public (Limited Distribution) (A-01-01-01018)</i>	December 2001

Status of Enumeration Task Force Recommendations

Status of Enumeration Task Force Recommendations	
Description of Recommendation	Status as of March 30, 2002
Provide refresher training on enumeration policy and procedures, with emphasis on enumerating non-citizens, for all involved staff.	Ongoing. Refresher training was conducted on December 19 and 20, 2001. Additionally, an interactive video training session was held on January 31, 2002. During the week of February 11, 2002, field office managers reviewed a daily maximum of 50 non-citizen enumeration actions. Managers provided feedback on problems or trends. Further action will be decided based on these findings, which were being evaluated at the time of this review.
Convene a joint task force between the Social Security Administration (SSA), the Immigration and Naturalization Service (INS), and the Department of State (DoS) to resolve issues involving enumerating non-citizens, including working out procedures for verifying INS documents before the Social Security number (SSN) is assigned.	<p>Ongoing. On January 3, 2002, SSA signed a protocol with the DoS outlining procedures for SSA use of information housed in the Refugee Data Center, which will be used to enumerate refugees. The procedure to verify immigration documents for refugees before assigning an SSN became effective in February 2002.</p> <p>SSA, INS, and DoS are also working together to implement the Enumeration at Entry program. Additionally, the INS has taken several steps to improve the timeliness of its data entry process. Once corrected, SSA will begin electronically verifying all non-citizen immigration documents before assigning an SSN. However, it is our understanding that corrections required by INS have been delayed. Therefore, SSA may not begin to implement this policy until late in Calendar Year 2002.</p>
Eliminate driver's licenses as a reason for a non-work SSN.	Completed. SSA notified the governors of all States in February 2002, and the policy went into effect on March 1, 2002.

<p>Provide an alternative to issuing a Numident printout for SSN verification.</p>	<p>Completed. The "NUMI-lite" went into production in SSA field offices in March 2002. This printout provides less identification information and therefore is less likely to facilitate identity theft.</p>
<p>Lower the age tolerance from 18 to 12 for mandatory interview procedures, including verification of birth records before enumeration for all applicants for original SSNs and require evidence of identity for all children, regardless of age.</p>	<p>Ongoing. The policy change needed to lower the age tolerance for mandatory interviews from 18 to 12 requires a regulatory change. Additionally, eliminating an existing waiver provision for those under age 7 will require a regulation. However, in the interim, SSA will rely on refresher training to strengthen existing policies. Beginning in May 2002, SSA will verify birth records for all applicants for original SSNs over the age of 1.</p>
<p>Determine the feasibility of photocopying (or scanning) all documentary evidence submitted with SSN applications.</p>	<p>Ongoing. Between February and March 2002, SSA conducted a pilot in two field offices to photocopy all evidence submitted in conjunction with SSN applications and ship them weekly to SSA's record storage facility for scanning. As of April 1, 2002, SSA was conducting the cost-benefit analysis for the pilot.</p>
<p>Change the Modernized Enumeration System to provide an electronic audit trail, regardless of the mode used to process SSN applications.</p>	<p>Completed. The audit trail went into production in mid-December 2001.</p>
<p>Implement the SSN Verification System.</p>	<p>Ongoing. SSA implemented a pilot of the on-line version in April 2002.</p>

Acronyms

DoJ	Department of Justice
DoS	Department of State
FBI	Federal Bureau of Investigation
INS	Immigration and Naturalization Service
OA	Office of Audit
OIG	Office of the Inspector General
SS	Social Security
SSA	Social Security Administration
SSN	Social Security Number

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kimberly A. Byrd, Director, Southern Audit Division, (205) 801-1605

Jeffrey Pounds, Deputy Director, Birmingham Field Office, (205) 801-1606

Staff Acknowledgments

In addition to those named above:

Kathy Buller, Counsel to the Inspector General

George Penn, Senior Attorney

Tom Sipes, Special Agent-in-Charge

Charles Lober, Senior Auditor

Kathy Youngblood, Senior Auditor

Susan Phillips, Auditor

Kimberly Beauchamp, Writer/Editor

For additional copies of this report, visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-1375. Refer to Common Identification Number A-08-02-22077.

DISTRIBUTION SCHEDULE

	<u>No. of Copies</u>
Commissioner of Social Security	1
Management Analysis and Audit Program Support Staff, OFAM	10
Inspector General	1
Assistant Inspector General for Investigations	1
Assistant Inspector General for Executive Operations	3
Assistant Inspector General for Audit	1
Deputy Assistant Inspector General for Audit	1
Director, Systems Audit Division	1
Director, Financial Management and Performance Monitoring Audit Division	1
Director, Operational Audit Division	1
Director, Disability Program Audit Division	1
Director, Program Benefits Audit Division	1
Director, General Management Audit Division	1
Team Leaders	25
Income Maintenance Branch, Office of Management and Budget	1
Chairman, Committee on Ways and Means	1
Ranking Minority Member, Committee on Ways and Means	1
Chief of Staff, Committee on Ways and Means	1
Chairman, Subcommittee on Social Security	2
Ranking Minority Member, Subcommittee on Social Security	1
Majority Staff Director, Subcommittee on Social Security	2
Minority Staff Director, Subcommittee on Social Security	2
Chairman, Subcommittee on Human Resources	1
Ranking Minority Member, Subcommittee on Human Resources	1
Chairman, Committee on Budget, House of Representatives	1
Ranking Minority Member, Committee on Budget, House of Representatives	1
Chairman, Committee on Government Reform and Oversight	1
Ranking Minority Member, Committee on Government Reform and Oversight	1
Chairman, Committee on Governmental Affairs	1

Ranking Minority Member, Committee on Governmental Affairs	1
Chairman, Committee on Appropriations, House of Representatives	1
Ranking Minority Member, Committee on Appropriations, House of Representatives	1
Chairman, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives	1
Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives	1
Chairman, Committee on Appropriations, U.S. Senate	1
Ranking Minority Member, Committee on Appropriations, U.S. Senate	1
Chairman, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate	1
Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate	1
Chairman, Committee on Finance	1
Ranking Minority Member, Committee on Finance	1
Chairman, Subcommittee on Social Security and Family Policy	1
Ranking Minority Member, Subcommittee on Social Security and Family Policy	1
Chairman, Senate Special Committee on Aging	1
Ranking Minority Member, Senate Special Committee on Aging	1
Vice Chairman, Subcommittee on Government Management Information and Technology	1
President, National Council of Social Security Management Associations, Incorporated	1
Treasurer, National Council of Social Security Management Associations, Incorporated	1
Social Security Advisory Board	1
AFGE General Committee	9
President, Federal Managers Association	1
Regional Public Affairs Officer	1
Total	97

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.

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 the Agency, as well as conducting employee investigations within OIG. Finally, OEO administers OIG's public affairs, media, and interagency activities 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.