OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

PERSONALLY IDENTIFIABLE INFORMATION MADE AVAILABLE TO THE GENERAL PUBLIC VIA THE DEATH MASTER FILE

June 2008 **A-06-08-18042**

AUDIT REPORT

Mission

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

Authority

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

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

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

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

Vision

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

SOCIAL SECURITY

MEMORANDUM

Date: June 4, 2008 Refer To:

To: The Commissioner

From: Inspector General

Subject: Personally Identifiable Information Made Available to the General Public Via the Death Master File (A-06-08-18042)

OBJECTIVE

Our objective was to determine the extent to which publication of the Death Master File (DMF) results in a breach of personally identifiable information (PII).

BACKGROUND

The Office of Management and Budget (OMB) defines PII as information that can be used to distinguish or trace an individual's identity, such as their name or Social Security number (SSN), alone, or when combined with other personal or identifying information linked or linkable to a specific individual, such as date and place of birth.[1] A heightened emphasis on PII protection has emerged as information technology and the Internet have made it easier to collect and disseminate this information. PII can also be exploited by criminals to stalk, or steal the identity of, a person or commit other crimes.

The expanded use of the SSN as a national identifier has given rise to individuals using SSNs belonging to others for illegal purposes. Stolen SSNs have been used to gain employment, obtain benefits and services, establish credit, and hide identities to commit various types of crimes. Identity theft affects millions of Americans each year. The Federal Trade Commission estimated total identity theft losses for businesses, financial institutions, and consumer victims totaled over $50 billion in 2002.[2] Preventing breaches of PII is essential to ensuring the Government retains the public's trust. Consequently, the Social Security Administration (SSA) is responsible for safeguarding PII in its possession. In May 2007, OMB issued a memorandum requiring that Federal

[1] OMB Memorandum M-07-16, page 1, footnote 1, dated May 22, 2007.

[2] *FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers,* http://www.ftc.gov/opa/2003/09/idtheft.shtm, Federal Trade Commission, Press Release, September 2003.

agencies develop and implement a PII breach notification policy.[3] The memorandum reemphasizes Federal agency responsibilities to appropriately safeguard PII, outlines incident reporting and handling requirements, and identifies factors to consider in determining when notification outside the agency should be given. The memorandum defined a breach as follows:

> …to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

The Death Master File

As a result of a *Freedom of Information Act* lawsuit,[4] SSA maintains a record of reported deaths known as the DMF. The terms of the related consent judgment required that SSA make available to the Plaintiff, the SSN, surname, and date of death of deceased numberholders. As of June 2007, the DMF database contained detailed information on more than 82 million numberholders. SSA provides DMF data to the Department of Commerce's National Technical Information Service (NTIS). NTIS, in turn, sells the DMF data to customers we broadly categorize as follows: (1) Federal, State, and local government customers; (2) industry customers including financial, investigative, credit reporting, and medical research organizations; and (3) public customers, including genealogists, individuals, etc. Customers can purchase the complete data file for $1,725 and subscribe to monthly electronic updates for another $2,600. The electronic updates provide subscribers with DMF additions, corrections, and deletions.

Customers use the DMF to verify identity as well as prevent fraud. By methodically running financial, credit, payment, and other applications against the DMF, users are better able to identify and prevent identity fraud. Further, some public customers purchase DMF information and make it available at no cost to the general public through the Internet.

The accuracy of death data is a highly sensitive matter for SSA. Erroneous death entries can lead to benefit termination, cause severe financial hardship and distress to affected individuals, and result in the publication of living individuals' PII in the DMF. When SSA becomes aware a death report was posted in error, SSA deletes the death entry from the DMF. Since January 2004, SSA has provided the Office of the Inspector General electronic files containing all updates made to the DMF. These files indicate, from January 2004 through April 2007, SSA deleted over 44,000 numberholders' death entries from the DMF. We did not verify whether the 44,000 individuals were alive at the time of our audit. However, SSA records indicated 20,623 of these individuals received SSA benefit payments in May 2007. The fact SSA paid benefits to individuals after deleting their death entries indicates SSA determined the individuals were alive.

[3] OMB M-07-16, supra.

[4] Perholtz v. Ross, Civ. No. 78-2385 and 78-2386 (D.D.C. - 1980).

Our review focused on these 20,623 individuals. (Additional background information is provided in Appendix B.)

RESULTS OF REVIEW

Since January 2004, SSA's publication of the DMF has resulted in the breach of PII for more than 20,000 living individuals erroneously listed as deceased on the DMF. SSA made these individuals' SSNs; first, middle, and last names; dates of birth and death; and State and zip codes of last known residences available to users of the DMF before learning they were not actually deceased. SSA attempted to retract these disclosures by deleting the individuals' information from the DMF. While these deletion transactions prevented the PII from being included in subsequent versions of the DMF, the deletions had no effect on the PII previously made available to DMF subscribers. In some instances, these individuals' PII remained available at the time of our audit for free viewing on the Internet. Public disclosure of living individuals' PII increases the opportunity for identity theft and subjects SSA to criticism from the affected individuals, the public and Congress and could subject SSA to legal action.[5]

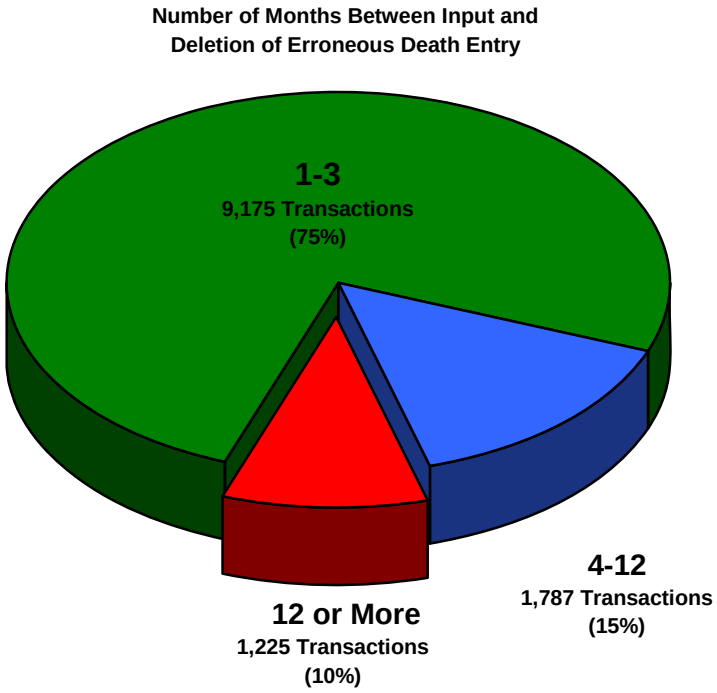
PUBLICATION OF THE DMF RESULTS IN PII BREACHES

SSA inadvertently exposed the PII of thousands of living individuals through publication of the DMF. SSA publishes deceased numberholders' personal information in the DMF. From January 2004 through April 2007, SSA processed transactions to delete erroneous death entries appearing on more than 44,000 numberholders' SSA records. However, in many cases, these deletion transactions did not occur until after the individual's PII was already exposed on the DMF. As of May 2007, SSA paid benefits to 20,623 of these numberholders, indicating SSA's acknowledgment the numberholders were alive.

Through review of available data, we identified both the death entry addition and deletion dates for 12,187 deletion transactions involving the 20,623 individuals in current payment status.[6] In 90 percent of the cases where these data were available, SSA deleted these individuals' erroneous death entries within 1 year of input.

[5] 5 U.S.C. § 552a(g)(1)(D).

[6] The remaining death entry addition dates were not recorded on available data files. We believed, but did not verify, this occurred either because the death entry was recorded before we began receiving monthly DMF transaction files or SSA processed the deletion transaction after, but in the same month as, the death entry.



SSA's policies and procedures openly acknowledge the occurrence of death reporting errors and state, "Occasionally, living individuals are erroneously included in the DMF (e.g., due to inaccurate death reports or inaccurate data input)."[7] Because SSA realizes it cannot guarantee the accuracy of information published in the DMF, it formally disclaims the accuracy of the DMF contents[8] and advises DMF customers/subscribers that not all information contained within is verified.

Because of the importance placed on privacy in the Social Security program, the first regulation adopted by the Social Security Board in June 1937 was Regulation Number 1,[9] which, to date, governs the privacy and disclosure of Social Security records. The Social Security Board found that the public interest required that confidential information in its possession, pertaining to any person, be preserved. Although SSA is aware it erroneously includes the PII of living individuals in the DMF, it continues to make the information available to the public. These actions not only appear to be contrary to Regulation 1, they also could cause the public to lose confidence in SSA's ability to protect sensitive information and subject SSA to civil litigation.

---

[7] SSA, POMS GN 03316.095.A, *Disclosure Without Consent to Recipients of the Death Master File (DMF) When Erroneous Death is Included on the DMF*.

[8] Id.

[9] 20 C.F.R. § 401 et seq.

DMF Deletion Transactions Did Not Remove PII from Public Domain

SSA's efforts to delete erroneous death entries from the DMF did not effectively mitigate the exposure of living individuals' PII. We randomly selected 250 instances where SSA deleted living individuals' death entries from the DMF. In September 2007, 4 to 43 months after SSA deleted the death entries, we searched at least one of the following three Internet sites that make DMF information available to the public at no charge to determine whether sampled individuals' PII remained accessible on the website.

- Rootsweb.com's Social Security Death Index at http://ssdi.rootsweb.com/
- Genealogy.com's Social Security Death Index at http://www.genealogy.com/genealogy/gen_ssdisearch.html
- Familysearch.org's Social Security Death Index at http://www.familysearch.org/ssdi/

Our review revealed that months[10] after SSA deleted the information from the DMF, the PII of 71 (28 percent) of the sampled living numberholders remained available for viewing on at least one of the Internet web sites. SSA action to remove erroneous death entries from the DMF did not prevent continued breaches of affected individuals' PII.

SSA staff stated that all purchasers of the DMF who continually use its data are advised, on the NTIS website, that it is mandatory that they keep their copy of the DMF up to date. SSA requires that they also purchase a subscription to the DMF updates and apply those updates. However, neither NTIS nor SSA enforced this requirement. SSA staff believed this oversight activity was an NTIS responsibility, particularly since NTIS receives all the fees associated with the sale of the DMF and from the update subscriptions. However, NTIS staff stated it provided no user oversight because the DMF was exclusively an SSA product. As a result, DMF purchasers did not always appear to abide by the update requirements, and the PII of living individuals remained publicly available, even long after SSA deleted the erroneous death entries.

Breach Notification Procedures Not Implemented When PII Exposed on the DMF

SSA did not implement PII breach notification procedures after becoming aware it erroneously published living numberholders' PII on the DMF. Further, SSA did not notify affected numberholders their PII was exposed on the DMF. OMB issued guidance requiring that Federal agencies report suspected or confirmed PII breaches to

[10] On average, the PII of these numberholders could be viewed on the Internet 30 months after SSA deleted the death entry from the DMF.

the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of discovery/detection.[11] This policy also outlines factors agencies should consider in determining when external breach notification should be given[12] and states

> Notification of those affected and/or the public allows those individuals the opportunity to take steps to help protect themselves from the consequences of the breach. Such notification is also consistent with the "openness principle" of the Privacy Act that calls for agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.[13]

SSA staff acknowledged the Agency does not implement any breach notification procedures when living individuals' personal information is erroneously published in the DMF. SSA staff reported that, relative to the total number of deceased individuals on the DMF (currently over 82.5 million) 20,000 DMF reporting errors represent an error rate of approximately .03 percent. SSA staff stated the DMF deletions discussed in the report occurred from January 2004 through April 2007; however, the OMB PII breach notification guidelines were not issued until May 2007.

We believe SSA's current practice is inconsistent with OMB guidance. For example, the OMB guidance states "[t]he magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification."[14] SSA should determine whether breach notification is warranted in accordance with the factors set forth in OMB guidance in instances where it erroneously publishes living numberholders' PII in the DMF.

Detailed Personal Information Published on the DMF

SSA discloses far more detailed personal information in the DMF than required under the original consent judgment that resulted in the creation of the DMF. Under the terms of the agreement, SSA was to compile a list that identified deceased numberholders' SSNs, surnames and dates of death. However, SSA expanded the information published in the DMF to include the decedent's date of birth, first and middle name, and last known residential state/zip code. According to SSA, the additional information became part of the DMF based on requests from subscribers. However, we could not confirm this because SSA did not maintain any supporting documentation.

---

[11] OMB M-07-16, supra, Attachment 2 § B.1. at page 10.

[12] OMB M-07-16, supra, Attachment 3 at page 12.

[13] OMB M-07-16, supra, Attachment 3 § A.3. at page 12.

[14] OMB M-07-16, supra, Attachment 3 § B.1b. at page 14.

In Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB directs agencies to reduce the volume of PII to the minimum necessary for the proper performance of a documented agency function, and to reduce the use of SSNs and to explore alternatives for use of SSNs as personal identifiers.[15] The *Social Security Act*[16] (Act) prohibits SSA from disclosing a person's death for purposes other than those enumerated in the Act if SSA's only source of that information was the State Death Match program. However, the Act allows, under certain circumstances, for SSA to share this restricted information with Federal and State agencies.[17] In these cases, SSA provides death information to other government agencies but does not publish death information in the public version of the DMF. Further restricting the amount of detailed personal information included in the DMF would reduce PII exposure—particularly in instances where living individuals' information is erroneously included—while allowing for the continued legitimate use of the valid death information.

CONCLUSION AND RECOMMENDATIONS

SSA's publication of the DMF resulted in the erroneous disclosure of thousands of living individuals' PII. SSA's attempts to mitigate these PII breaches were not always effective in removing the PII from the public domain. SSA did not notify either US-CERT or the affected individuals upon learning the Agency had erroneously included living individuals' PII in the DMF. Further, SSA discloses far more detailed personal information in the DMF than required by the consent agreement that resulted in the creation of the DMF. With the growing use of the Internet—and the public and Congress' concerns with identity theft and the disclosure of personal information—SSA must prevent the improper disclosure of PII by ensuring the DMF does not contain the PII of living individuals before making the information available to the general public.

Publication of the DMF involves the inherent risk living individuals' PII will be mistakenly breached. If SSA continues to publish the DMF with the knowledge its contents cannot be guaranteed as accurate and contain the PII of living numberholders, we recommend SSA:

1. Work with the Department of Commerce to implement a risk-based approach for distributing DMF information. For example, SSA could request that NTIS delay release of DMF updates to public customers by at least 1 year to give SSA time to correct most, if not all erroneous death entries.

2. Limit the information included in the DMF version sold to public customers to the absolute minimum required and explore alternatives to inclusion of the full SSN.

---

[15] OMB M-07-16, supra, Attachment 1 §§ B.1.a. at page 6 and B.2.a. and b at page 7.

[16] The *Social Security Act* § 205(r)(6), as amended, 42 U.S.C § 405(r)(6).

[17] The *Social Security Act* §§ 205 (r)(3)-(5), as amended, 42 U.S.C. §§ 405(r)(3)-(5).

3. Initiate required breach notification evaluation procedures, in accordance with OMB guidance, upon notification that SSA mistakenly included living individuals' PII in the DMF.

4. Provide appropriate notification, as determined by applying OMB guidance, to living individuals whose PII was released in error, and advise them to take appropriate steps to prevent further compromise of their personal information.

AGENCY COMMENTS

SSA agreed in general with Recommendations 1, 3, and 4, and stated it would consider implementing Recommendation 2. SSA recognizes the undue hardship individuals may experience when their personal information is erroneously compromised and is fully committed to finding ways to reduce any risk of PII exposure. SSA also stated it must balance these hardships against potential economic impact further restrictions on DMF information could have on public and private users. Further, SSA stated it faces several challenges to limiting the DMF information it provides. SSA stated that, in April 2008, it convened a task force to identify options to improve the death reporting process. SSA's comments are included in Appendix D.

On May 14, 2008, the Office of the Chief Information Officer informed us that SSA recently submitted a list to US-CERT identifying thousands of names erroneously included in the DMF. In addition, SSA provided US-CERT a separate list with the names of hundreds of individuals whose erroneous death entries were removed from the DMF the previous week.

OIG RESPONSE

We appreciate SSA's agreement with Recommendations 1, 3, and 4 and its consideration to implement Recommendation 2. We encourage SSA to address these issues as expeditiously as possible. In addition to responding to the recommendations, SSA also provided technical comments and we incorporated these as we believed appropriate.

Patrick P. O'Carroll, Jr.

Appendices

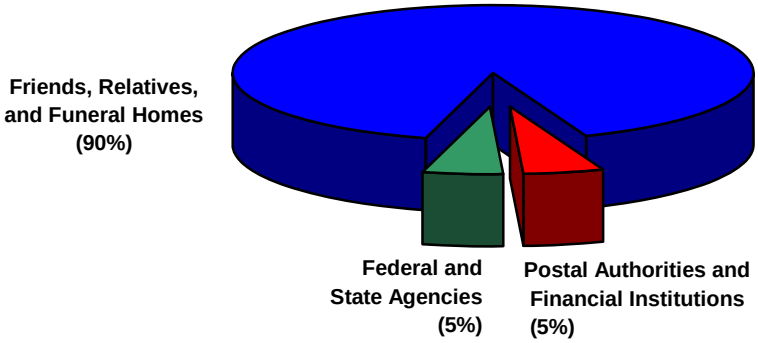
Acronyms

Act	*Social Security Act*
DMF	Death Master File
NTIS	National Technical Information Service
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POMS	Program Operations Manual System
SSA	Social Security Administration
SSN	Social Security Number
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Background

As depicted below, the Social Security Administration (SSA) receives most death reports from funeral homes or friends/relatives of the deceased. SSA considers such first-party death reports to be verified and immediately posts them to the Death Master File (DMF).

SSA SOURCES FOR DEATH REPORTS



Other sources of death reports include States and other Federal agencies as well as Postal authorities and financial institutions. SSA immediately posts non-beneficiary information received from these sources to the DMF without verification. However, if these reports indicate an SSA beneficiary died, SSA requires additional verification before terminating benefits or posting the death entry to the DMF.[1] Verification of death means that a reporter (usually someone in the person's home, a representative payee, a nursing home, a doctor, or hospital) agrees the person is deceased and, if the date of death is an issue, corroborates the reported date of death.[2]

[1] SSA POMS, GN 02602.050A, *Processing Reports of Death*.

[2] SSA POMS, GN 02602.050A.2.

Scope and Methodology

To accomplish our objective, we:

- Reviewed Federal laws on disclosure of personal information.
- Reviewed Office of Management and Budget guidance on *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* as well as the Social Security Administration's (SSA) policies and procedures related to erroneous death terminations and release of personally identifiable information.
- Interviewed SSA Systems and Operations staff to discuss procedures used to remove an erroneous death entry from a wage earner's record.
- Interviewed the Department of Commerce's National Technical Information Service (NTIS) staff to discuss NTIS' role in selling and distributing the Death Master File (DMF).
- Analyzed 46,035 instances where SSA removed death entries from the DMF during the period January 2004 through April 2007. We identified 21,213 deletions from the DMF (representing 20,623 numberholders) for beneficiaries/recipients who were receiving benefits as of April and May 2007.
- Analyzed time between the addition to the DMF and the deletion from the DMF for 12,187 of 21,213 resurrection transactions (death entry addition dates were not recorded on available data files for the remaining 9,026 cases).
- In September 2007, we selected a random sample of 250 of the 21,213 resurrection transactions. For each sampled individual, we searched free Internet web sites to determine if the living beneficiaries' personal identifying information could be viewed.

We performed our audit from August through October 2007 at SSA's Regional Office in Dallas, Texas. We did not test the general or application controls of SSA systems that generated electronic data used for this audit. Instead, we performed other validation tests and found the data to be sufficiently reliable to meet our audit objectives. The entity audited was the Office of the Deputy Commissioner for Operations. We conducted this audit in accordance with generally accepted government auditing standards.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: May 6. 2008 Refer To: S1J-3

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

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

Subject: Office of the Inspector General (OIG) Draft Report, "Personally Identifiable Information Made Available to the General Public Via the Death Master File" (A-06-08-18042)-- INFORMATION

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

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

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "PERSONALLY IDENTIFIABLE INFORMATION MADE AVAILABLE TO THE GENERAL PUBLIC VIA THE DEATH MASTER FILE" (A-06-08-18042)

Thank you for the opportunity to review and comment on the draft report. We fully recognize the undue hardship that individuals may experience when their personal information is erroneously compromised. We are therefore fully committed to find ways to reduce any risk of PII exposure. As we assess this issue, we strongly caution the OIG against releasing this report publicly. We believe limited distribution would be more responsible. We recognize that this information may already be known to some, but this report highlights the issue and could encourage misuse.

As we strive to ensure the accuracy of the information we receive, we must also comply with our responsibility to satisfy the *Perholtz* court order. The *Perholtz* case, a Freedom of Information Act (FOIA) lawsuit, resulted in a consent judgment that required us to make available the full SSN, surname, and date of death of deceased number holders, thus creating the Death Master File (DMF). Oversight organizations and Congress later recognized the immense value of the DMF in preventing fraud and erroneous payments, by sharing the information of deceased individuals. As you cite in your report, identity theft costs businesses, financial institutions and consumer victims more than $50 billion in a single year. The DMF is an extremely effective tool that saves many public and private entities billions of dollars each year.

We have already begun in depth analysis to pinpoint the size of the PII exposure problem and the source of erroneous data. We have found that the DMF is 99.59 percent accurate. Of 2.5 million death reports added each year, the DMF reflects approximately 9,000 of these are erroneous cases, an error rate of .0041, or less than one half of one percent. A nation-wide implementation of the Electronic Death Registration (EDR) process would eliminate the vast majority of these erroneous reports.

EDR is a fully automated data exchange that allows states to transmit death reports directly to SSA. EDR has slowly expanded on a state by state basis over the past four years, and currently 23 states/jurisdictions participate. EDR transactions are virtually error free. Generally, it takes about two years for a State to fully rollout the process state-wide. EDR nation-wide roll-out is contingent on Congressional funding of the Department of Health and Human Services (HHS) so that they in turn can fund States through a grant process. The Intelligence Reform and Terrorist Prevention Act of 2004 transferred the funding of EDR to HHS. To date, the lack of funding has been the main barrier to full expansion.

However, we are not waiting for the nation-wide roll-out to address this small but critical error rate. We have been striving to close the very small but important error rate in the DMF by other means. We know that the primary source of error in the DMF is manual inputs done in our field offices and teleservice centers. Of an approximate 1.5 million death reports manually input, errors result on about 7,000 inputs. Although the overall accuracy rate on these manual inputs is still over 99.5%, we have sought ways to prevent all error. In July 2007, we implemented a computer screen alert, as a double check for our employees to ensure they are taking the proper

action. We also issued clearer instructions and conducted training sessions. We have seen a significant reduction in error as a result of that change. We are also looking closely at several additional systems enhancements that could potentially tighten our field office and teleservice processes to reduce error. While we are eager to find and pursue any other methods to further ensure accuracy, it is difficult to eliminate all error in a manual system. To reiterate, EDR would be the most effective solution.

Recommendation 1

Work with the Department of Commerce to implement a risk-based approach for distributing DMF information. For example, we could request that the National Technical Information Service delay release of DMF updates to public customers by at least 1 year to give us time to correct most, if not all erroneous death entries.

Response

We agree to explore any possible risk-based options for distributing DMF information. We also agree, as noted in your report that we should seek ways to ensure that purchasers and users of the DMF keep their file up to date.

While we are willing to explore options, we believe that any delay in release of the DMF will cause significant economic hardship to public and private entities and impede their ability to deter fraud, waste and abuse. A 2001 GAO audit noted that "*timely receipt of death information and prompt updating of financial data are key factor's in the financial industry's ability to prevent fraud and identity theft involving the SSN's of deceased individuals*." That GAO report recommended that SSA distribute the DMF more frequently to help entities to prevent fraud and identity theft. (See GAO 2001 audit "Observations on Improving the Distribution of Death Information". http://www.gao.gov/new.items/d02233t.pdf.) We now release updates weekly.

Further, there have been numerous individuals who have testified before Congress regarding the importance of the DMF. In 2001, the Financial Services Coordinating Committee, or FSCC, testified. FSCC represents the largest and most diverse group of financial institutions in the country, including the American Bankers Association, American Council of Life Insurers, American Insurance Association, Investment Company Institute, and Securities Industry Association. FSCC noted that, "*A key method for preventing fraud and identity theft due to the misuse of a SSN is to identify the fraudulent use of a deceased individual's SSN. The linchpin of this prevention effort is the SSA's DMF*."
http://waysandmeans.house.gov/Legacy/socsec/107cong/11-8-01/11-8duge.htm

Also, any delay in the DMF would likely prompt organizations to request the information under the Freedom of Information Act (FOIA). We are required to respond to FOIA requests within 20 business days.

Recommendation 2

Limit the information included in the DMF version sold to public customers to the absolute minimum required and explore alternatives to inclusion of the full SSN.

Response

We are considering limiting the information included in the DMF version sold to the public to the absolute minimum required. We will also explore alternatives to the use of the full SSN.

We face several challenges to limiting the information we provide. First, we believe there is a strong likelihood of litigation under FOIA if we were to reduce the amount of information currently on the DMF. If we removed any data from the DMF, any FOIA requester could seek to have it included again. Without valid legal basis to withhold under FOIA, we would again be faced with the need to add the information or face litigation. Also, limiting the DMF to minimum numbers of data elements would greatly reduce its utility for fighting identity theft and fraud. Failure to supply the full SSN for individuals on the DMF would negate the positive cost-saving results achieved by many public and private entities.

There are additional challenges we face with regard to finding an alternative to the SSN. First, we are bound by a consent decree which requires us to include the full SSN. Second, the users of the DMF rely on the SSN to match our records with theirs.

Recommendation 3

Initiate required breach notification evaluation procedures, in accordance with the Office of Management and Budget's (OMB) guidance, upon notification that we mistakenly included living individuals' PII in the DMF.

Response

This is a unique and complex issue. While we recognize the small percentage of error in the DMF, we are concerned with the characterization of those errors as "PII breaches." Nonetheless, we will take a cautious approach and initiate breach notification evaluation procedures in accordance with OMB guidance.

For many years, SSA, GAO, OIG, electronic privacy advocacy groups and other oversight entities have fully understood that the DMF contains a small degree of error. In fact, SSA specifically requires that a disclaimer accompany the distribution of DMF as follows, "*SSA cannot guarantee the accuracy of the DMF. Therefore, the absence of a particular person on this file is not proof that the individual is alive. Further, in rare instances it is possible for the records of a person who is not deceased to be included erroneously in the DMF*." To the best of our knowledge, none of these entities had characterized the DMF errors as a PII breach prior to this audit report. To the contrary, these entities have repeatedly highlighted the importance of the DMF as a tool to prevent fraud, abuse and billions of dollars in erroneous payments annually (see GAO report cited in response 1 above).

In addition, to the best of our knowledge, no case of fraud or abuse has occurred as a result of errors in the DMF. This may be largely due to the fact that living persons erroneously placed in the DMF are reported as being deceased. Therefore, it is difficult for identity thieves to distinguish these records from other deceased individuals in the DMF. It would also be difficult to abuse that PII because banks, credit bureaus and other agencies would block activity on that particular SSN, assuming the individual to be deceased. Further, when an individual notifies SSA that our records reflect an erroneous death, we take immediate action to correct our records and the DMF.

In April 2008, we convened a task force to identify options to further improve the death reporting process. This task force is assessing the notification and remediation practices under OMB guidelines. Meanwhile, we will continue to release the DMF weekly, despite the small error rate because any delay in the release of the DMF would impede private and public organizations' ability to prevent fraud, abuse and billions of dollars in erroneous payments.

Recommendation 4

Provide appropriate notification, as determined by applying OMB guidance, to living individuals whose PII was released in error, and advise them to take appropriate steps to prevent further compromise of their personal information.

Response

We agree that the Agency will apply the OMB guidance and provide notification as appropriate, based on the OMB guidance. We currently provide notice to individuals when we make a death status correction in our records and in the DMF.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Ron Gunia, Director, Dallas Audit Division, (214) 767-6620

Jason Arrington, Audit Manager, (214) 767-1321

Acknowledgments

In addition to those named above:

Clara Soto, Senior Auditor

Erica Turon, Senior Analyst

Brennan Kraje, OIG Statistician

Chuck Zaepfel, Information Technology Specialist

For additional copies of this report, please visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-06-08-18042.

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, Committee on the Budget, House of Representatives

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

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 Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Chief Counsel to the Inspector General (OCCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

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

Office of Investigations

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

Office of the Chief Counsel to the Inspector General

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

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.