

This Testimony is Embargoed Until Thursday, February 2nd at 9:00 AM

U.S. House of Representatives

**Committee on Ways and Means
Subcommittee on Social Security**



Statement for the Record

Hearing on Social Security's Death Records

**The Honorable Patrick P. O'Carroll, Jr.
Inspector General, Social Security Administration**

February 2, 2012

Good morning, Chairman Johnson, Ranking Member Becerra, and members of the Subcommittee. It is a pleasure to appear before you, and I thank you for the invitation to testify today. I have appeared before Congress many times to discuss issues critical to the Social Security Administration (SSA) and the services the Agency provides to American citizens; I appeared before the Subcommittee last week to discuss SSA's Disability Insurance program. Today, we are discussing SSA's Death Master File (DMF) and the Agency's process for distributing death records.

SSA has, on the Numident—the Agency's master database of Social Security number (SSN) holders—a record of reported deaths. Because of a 1978 *Freedom of Information Act* (FOIA) lawsuit—*Perholtz vs. Ross*—SSA in 1980 was required to make available to the public death records that included the SSN, the last name, and the date of death of deceased number holders; the result was the creation of the DMF, an extract of Numident data. Each DMF record usually includes the following: SSN, full name, date of birth, and date of death. The file contains about 85 million records, and it adds about 1.3 million records each year. SSA receives death information from many sources, including family members, funeral homes, and some (but not all) States. SSA does not have a death record for all deceased individuals, thus SSA does not guarantee the file's veracity. A person's absence from the file does not guarantee the person is alive.

SSA provides the DMF to the Department of Commerce's National Technical Information Service (NTIS), a cost-recovery agency, which, in turn, sells DMF data to public and private industries—government, financial, investigative, credit reporting, and medical customers. Those customers use the data to verify death and to prevent fraud, among other uses. The DMF thus contains more information than required by the *Perholtz* ruling.¹

The public distribution of SSA's death records and personally identifiable information (PII) raises concerns related to SSN misuse and identity theft. Your Subcommittee has discussed ways to improve SSN protection with SSA and the Office of the Inspector General (OIG) before, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft persists. We in the OIG are well aware of the central role the SSN plays in American society, and part of our mission is to protect its integrity. Therefore, while limiting or discontinuing the DMF's availability is ultimately a legislative and policy decision for the Congress and SSA to make, the OIG has long taken the position that to the extent possible, public access to the DMF should be limited to that required by law, and that all possible steps should be taken to ensure its accuracy. We have made numerous recommendations to this effect.

The Congress has recognized the importance of this issue, as current bills for consideration address access to the DMF. Chairman Johnson and several members of your Subcommittee in November 2011 introduced the *Keeping IDs Safe Act*, which would end the sale of the DMF. While some government and law enforcement agencies would still have access to the file to combat fraud, the bill would help protect the death data of all number holders.

¹ In November 2011, SSA made a change to DMF records it provides to NTIS. The *Social Security Act* prohibits SSA from disclosing State death records the Agency receives through its contracts with the States, except in limited circumstances. SSA thus removed about 4.2 million State death records from the DMF. SSA currently distributes Numident data under agreements with eight government agencies, including the Centers for Medicare & Medicaid Services and the Internal Revenue Service.

Another House bill, introduced in October 2011 to prevent identity theft and tax fraud, calls for the Commerce Department to develop a certification program for individuals to complete before accessing the DMF. According to the proposal, any certified person who disclosed DMF data to another individual, or any certified person who misused the data, would be fined \$1,000 for each illegal disclosure or use.

The DMF data has important and productive uses. Medical researchers and hospitals track former patients for their studies; investigative firms use the data to verify deaths related to investigations; and pension funds, insurance organizations, and Federal, State, and local governments need to know if they are sending payments to deceased individuals. The financial community and State and local governments can identify and prevent identity theft by running financial and credit applications against the DMF. However, in the form in which the DMF is currently distributed, methods exist for individuals to misuse SSNs and commit identity theft. We have made recommendations to SSA that would improve the protection of PII available in the DMF through both decreased inclusion of data and increased accuracy; SSA has agreed with some of our recommendations and disagreed with others.

Our March 2011 report, *Follow-up: Personally Identifiable Information Made Available to the Public via the Death Master File*, examined whether SSA took corrective actions to address recommendations we made in a June 2008 report on the DMF. In the June 2008 report, we determined that, from January 2004 through April 2007, SSA's publication of the DMF resulted in the potential exposure of PII for more than 20,000 living individuals erroneously listed as deceased on the DMF. In some cases, these individuals' PII was still available for free viewing on the Internet—on ancestry sites like ancestry.com and familysearch.org—at the time of our report.

In June 2008, we recommended that SSA:

1. Work with the Commerce Department to implement a risk-based approach for distributing DMF information, such as implementing a several-month delay in the release of DMF updates, so that SSA could correct erroneous death entries;
2. Limit the amount of information included on the DMF to the absolute minimum required, and explore alternatives to the inclusion of an individual's full SSN;
3. Initiate required breach notification procedures upon learning that the Agency mistakenly included living individuals' PII in the DMF; and
4. Provide appropriate notification to living individuals whose PII was released in error.

In our March 2011 report, we found that SSA had taken actions on recommendations 3 and 4. SSA implemented procedures to report erroneous death entry-related PII breaches to the Department of Homeland Security's U.S. Computer Emergency Readiness Team each week. The Agency also hired a contractor to provide ongoing reviews of DMF exposure related to thousands of individuals whose PII was inadvertently exposed from July 2006 through January 2009. The contractor evaluated available data for patterns that could identify organized misuse, and according to SSA, as of March 2011, the contractor identified no PII misuse. Thus, SSA did not provide breach notifications to any individual number holders. We recommended that SSA notify *all* individuals whose PII was exposed, regardless of the detection of PII misuse.

SSA did not take actions on recommendations 1 and 2. SSA did not implement a delay in the release of DMF updates, as the Agency indicated that public and private organizations rely on the DMF to combat fraud and identity theft. To be effective, those organizations must have immediate and up-to-date information, SSA said. The Agency also did not attempt to limit the amount of information included on the DMF, and it did not explore alternatives to the inclusion of an individual's full SSN, citing the *Perholtz* consent judgment and potential litigation under FOIA. SSA added that a deceased individual does not have a privacy interest, according to FOIA.

Our March 2011 follow-up review revealed that in addition to the recommendations with which SSA did not agree, several issues remained:

- SSA continued to, inadvertently, expose the PII of thousands of living individuals each year, because the Agency released death information without a short delay to identify and correct most death-report errors.
- SSA's efforts to delete erroneous death entries from the DMF did not completely mitigate the exposure of living individuals' PII. At the time of the report, we searched several ancestry Websites, like familysearch.org, and there were instances in which living individuals' PII remained accessible. This likely occurred because the Website was not timely processing DMF updates.
- SSA continued to disclose far more detailed PII in the DMF (including first name, middle name, and date of birth) than required under the original *Perholtz* consent judgment. We continue to believe that reducing the amount of detailed PII included in the DMF would allow the continued legitimate use of valid death information, while at the same time limiting the inadvertent PII exposure of living individuals.

According to SSA, there are about 1,000 cases each month in which a living individual is mistakenly included in the DMF. SSA said that when the Agency becomes aware it has posted a death report in error, SSA moves quickly to correct the situation, and the Agency has not found evidence of past data misuse. However, we remain concerned about these errors, because erroneous death entries can lead to benefit termination and cause severe financial hardship and distress to affected individuals. We also have concerns that DMF update files, some with active SSNs, are a potential source of information that would be useful in perpetrating SSN misuse and identity theft, including the theft of child identities. DMF updates can reveal to potential criminals the PII of individuals who are still alive.

We have several other ongoing reports related to DMF data:

- In *Title II Deceased Beneficiaries Who Do Not Have Death Information on the Numident*, we have identified about 1.2 million Title II beneficiaries who have a date of death on the Master Beneficiary Record (MBR), but they do not have death information on SSA's Numident. SSA uses death information from the Numident to create the DMF. If a person knew an individual was deceased and that the death record was not on the Numident, the person could use the deceased's information to fraudulently file for benefits or credit.
- In *Deceased Beneficiaries Who Have Different Dates of Death on the SSA's Numident and Payment Records*, we identified about 11,000 deceased beneficiaries who have a date of death on the Numident that differs by at least one month from the date of death on the MBR or Supplemental Security Income Record (SSR). We also identified 39 cases in which the date discrepancies resulted in potential improper payments of more than \$72,000.

- In *Using Medicare Claim Data to Identify Deceased Beneficiaries*, we will match SSA beneficiary records with CMS databases containing Medicare non-utilization information to determine if the beneficiaries are alive.

We in the OIG also remain concerned with the overall accuracy of SSA's death data. SSA receives about 2.5 million death reports each year from many sources, including family members and funeral homes. In addition, to identify improper payments to deceased beneficiaries, SSA has computer matches of death information from other Federal Agencies, such as the Department of Veteran Affairs. However, before SSA can terminate benefits based on a computer match, it must verify the accuracy of the death information.

SSA has worked with the National Association for Public Health Statistics and Information Systems to develop standards and guidelines for a nationwide system of electronic death registration (EDR), and Congress authorized the Department of Health and Human Services to provide grants to help States set up their systems. Under EDR, SSA verifies the decedent's name and SSN with the State at the beginning of the death registration process, thereby allowing SSA to take immediate action to terminate benefits without needing to verify the accuracy of the death report. Currently 32 States, the District of Columbia, and New York City have implemented EDR. SSA expects to work with eight additional States that plan to implement EDR over the next two years.

We have conducted several audits in recent years related to the accuracy of DMF data:

- In a September 2011 report, we found that SSA paid \$644,000 in monthly survivor benefits to family members of 642 living (but mistakenly listed on the DMF) wage earners, even though the Agency had deleted the wage earners' death entries from the DMF, and SSA's Numident file indicated the wage earners were still alive.
- An April 2011 report found SSA needed to improve controls to ensure it takes timely and proper actions to resolve death information on the Numident for suspended Title II beneficiaries.
- We found that SSA issued payments to deceased beneficiaries after recording valid dates of death on the beneficiaries' Numident record in June 2009.
- In February 2009, we found that about 98 percent of erroneous death entries on the DMF were death reports from non-State sources. Therefore, even if all States were to submit death reports via EDR, there could still be some erroneous death entries on the DMF. We also found that some death-reporting errors occurred for EDR States.

In conclusion, the OIG has conducted, and continues to conduct, significant audit work to identify methods SSA could implement to protect PII and death data and to improve the accuracy of its death reporting. While we encourage efforts to limit public access to this data through legislative or policy changes (such as the *Keeping IDs Safe Act*), barring such changes, SSA should implement a risk-based approach for distributing DMF information, and the Agency should attempt to limit the amount of information included on the DMF. These actions would protect PII and potentially limit the misuse and abuse of SSNs and identity theft.

We will continue to provide information to SSA's decision-makers and to your Subcommittee, and we look forward to assisting in this effort and future efforts. Thank you again for the invitation to be here today. I would be happy to answer any questions.