SOCIAL SECURITY'S DEATH RECORDS

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 2, 2012

Serial No. 112–SS13

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
78–179 WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

KEVIN BRADY, Texas
PATRICK J. TIBERI, Ohio
AARON SCHOCK, Illinois
RICK BERG, North Dakota
ADRIAN SMITH, Nebraska
KENNY MARCHANT, Texas

XAVIER BECERRA, California, *Ranking*
LLOYD DOGGETT, Texas
SHELLEY BERKLEY, Nevada
FORTNEY PETE STARK, California

Jon Traub, *Staff Director*
Janice Mays, *Minority Chief Counsel*

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

SOCIAL SECURITY'S DEATH RECORDS

THURSDAY, FEBRUARY 2, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:09 a.m., in Room B318, Rayburn House Office Building, Hon. Sam Johnson [Chairman of the Subcommittee] presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
Thursday, February 2, 2012
SS–13

CONTACT: (202) 225–1721

Chairman Johnson Announces a Hearing on Social Security's Death Records

U.S. Congressman Sam Johnson (R–TX), Chairman of the House Committee on Ways and Means Subcommittee on Social Security announced today that the Subcommittee will hold a hearing on the accuracy and uses of the Social Security Administration's Death Master File. **The hearing will take place on Thursday, February 2, 2012 in B–318 Rayburn House Office Building, beginning at 9:00 a.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Subcommittee and for inclusion in the printed record of the hearing.

BACKGROUND:

The Social Security Administration (SSA) collects death information to administer its programs. Approximately 2.5 million death reports are received each year from relatives, friends, funeral homes, financial institutions, postal authorities, States and Federal agencies. Verified death information is then used to stop benefits to those who have died and provide benefits to surviving spouses and children.

A 1980 Freedom of Information Act (FOIA) court-mandated settlement required the SSA to make publicly available the surname, Social Security Number (SSN) and date of death of deceased SSN holders. As a result, the SSA created the Death Master File (DMF), a file of all deaths reported to the SSA since 1936 from sources other than States. The public file includes 84 million records and approximately 1.5 million records are added each year. At subscriber request, the file also includes date of birth and first and middle name for each SSN holder, in addition to the information required under the settlement.

The SSA makes the DMF, often referred to as the Public DMF, available to the National Technical Information Service (NTIS) of the Department of Commerce through a contractual agreement. There is a broad commercial interest in the DMF to prevent fraud, waste, abuse and identity theft. NTIS sells the DMF to private and public sector customers, including government agencies, financial institutions, investigative entities, credit reporting organizations, medical researchers, genealogical researchers and other industries. Workers' compensation, pension, annuity, unemployment and other benefit plans use the DMF to detect improper payments sent to those who are deceased.

In 1983, Congress amended the Social Security Act (P.L. 98–21) to require the SSA to enter into contractual agreements to obtain death records from States, established the conditions under which the SSA may provide State information to other Federal and State agencies and exempted death reports the SSA receives from the States from disclosure under FOIA.

States play a key role in the death reporting process. The SSA is working with States who are building a streamlined death registration process known as Electronic Death Registration (EDR).

Certain death records that appeared to be coming from non-State independent sources but were in fact State EDR data were for years included in the DMF. Following a recent review of the EDR, the SSA determined that as of November 1, 2011, all death records received through the EDR will be removed from the DMF. It is expected that as the use of the EDR expands through the States, the mandated FOIA settlement will apply to less death information and the number of records that may be entered on the DMF will be further reduced.

As many news reports have accounted, incorrect death reports have created severe personal and financial hardship for those who are erroneously listed as deceased, including the termination of benefits and the public disclosure of information that the SSA normally keeps confidential. According to the SSA, each year approximately 14,000 individuals are incorrectly listed as deceased on the DMF. Those affected have experienced termination of benefits, rejected credit, declined mortgages and other devastating consequences while their personal and private information is publicly exposed.

Further, the DMF reportedly has become a source for thieves to capitalize on the identities of children and others who have died. Criminals appear to be exploiting the easy access to death information to submit fraudulent tax returns that include the decedent's SSN. Parents of the deceased child do not know their child's identity has been stolen until the IRS rejects their legitimately filed return and the theft has been exposed. In fact, "The National Taxpayer Advocate's 2011 Annual Report to Congress," released on December 31, 2011, included a section entitled "The Federal Government Facilitates Tax-Related Identity Theft by Publicly Releasing Significant Personal Information of Deceased Individuals."

In announcing the hearing, Chairman Sam Johnson (R–TX) stated, **"Since 1980, Social Security has been required to publicly make available Americans' personal information through the so-called Death Master File. Nearly anyone can get this information, including identity thieves. Identity theft affects swindled businesses, American taxpayers and grieving families. Also any one of us could find ourselves on that list by mistake—a mistake which could cause severe financial hardship. Americans deserve better so I introduced H.R. 3475, the 'Keeping IDs Safe Act of 2011,' a bill that would stop Social Security from making this information public."**

FOCUS OF THE HEARING:

The hearing will focus on the history, accuracy, use and impacts of the Death Master File along with options for change.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, *http://waysandmeans.house.gov*, select "*Hearings*." Select the hearing for which you would like to submit, and click on the link entitled, "*Click here to provide a submission for the record*." Once you have followed the online instructions, submit all requested information. ***ATTACH*** your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, **by the close of business on Tuesday, February 16, 2012**. **Finally**, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225–1721 or (202) 225–3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word format and MUST NOT exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission listing the name, company, address, telephone, and fax numbers of each witness.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available on the World Wide Web at *http://www.waysandmeans.house.gov*.

Chairman JOHNSON. We are going to sit here for a few minutes. Our guys went to a prayer breakfast this morning, some of them, and they are on the way, but not here yet. And legally we can't start a hearing without at least two of us. And so as soon as someone arrives, we will let Mr. Astrue begin his remarks. Until then, don't attack him.

[Laughter.]

Okay, we have another Member, Mr. Marchant.

Mr. MARCHANT. Good morning. Sorry, I got turned around in the basement.

[Laughter.]

Chairman JOHNSON. Did you? I get lost over here, too.

Well, since my fellow Texan has arrived, we will begin the hearing. I want to thank all of you for being here this morning. The hearing will come to order.

Social Security has always collected death information so it can stop benefits to those who have died and start benefits for their survivors. Today about 2.5 million death reports are received from many sources, including families, funeral homes, hospitals, financial institutions, States and Federal agencies. Social Security shares death records with other Federal benefit-paying agencies, like the Veterans Administration, for instance.

The 1980 Freedom of Information Act court-mandated settlement required Social Security to also make information about deceased Social Security number holders available to the public. Under the Freedom of Information Act, deceased individuals have no privacy rights, so their personal information can be disclosed. In response, Social Security created the so-called Death Master File. Soon afterward, in 1983, Congress changed the law to protect death reports received from States. The information in the Death Master File comes from non-State sources and the file is sold to the public by the Department of Commerce.

Over time, a broad commercial interest has developed in the Death Master File for use in private benefit management and as a tool to prevent fraud and identity theft. Many groups purchase

the file from the Commerce Department, including government agencies, credit reporting agencies, financial institutions, law enforcement organizations, and medical and genealogical researchers.

But what made sense 30 years ago, no longer makes sense today. Identity thieves who get their hands on a Social Security number can reap instant rewards, while the rightful owner has no idea what has happened. And that is partly due to our technology today.

With 84 million listed individuals and 1.5 million new individuals added each year, it appears that this File has become a resource for criminals seeking to capitalize on Americans' identities, particularly the identities of deceased children.

In her recent annual report to Congress, the National Taxpayer Advocate found that the Federal Government facilitates tax-related ID theft through the release of the Death Master File. In no uncertain terms, the National Taxpayer Advocate states in the report that she "is appalled that the Federal Government is making sensitive personal information so readily available, when such information can easily be used to commit identity theft."

We will hear the heartbreaking story of the Agin family, whose four-year-old daughter had her identity stolen shortly after she passed away. Only when their tax return was rejected by the IRS, did they learn that an identity thief had already filed a return claiming their child as a dependent.

Worrying about a lost loved one's Social Security number is a burden no grieving family should bear. That's why I, along with a number of my colleagues, introduced H.R. 3475, the "Keeping IDs Safe Act of 2011," to protect this information. Even Social Security reports that approximately 14,000 living individuals are wrongly placed on the Death Master File each year. Any one of us could find ourselves mistakenly on that list—an inexcusable mistake that exposes our personal information and could cause severe personal and financial hardship.

Through our witnesses today we will learn more about the history of the Death Master File, its accuracy, and how it is used. Soon this Subcommittee will hold a joint hearing with the Ways and Means Oversight Subcommittee to more closely examine identity theft in the tax system.

Americans rightfully deserve action to stop thieves from exploiting our deceased loved ones.

Do you have any comments to make before we allow your witness to make his opening remarks?

Mr. MARCHANT. Well, thank you, Mr. Chairman. I have looked forward to this hearing for some time. I apologize for being late.

This issue really came to the forefront in my mind a couple of years ago, when I had a family contact me about the theft of their Social Security card from their mailbox for an infant that was just born. And of course, that does not parallel the tragedy of a child that has died having their Social Security number stolen, but this family was very distraught. And I became distraught as well, when I contacted the Social Security Administration on their behalf and was told that, unless we could prove that the child had come to some financial harm, they would not be able to be issued a new Social Security card or a new number.

I understand that a person that has had several jobs or has had a credit report and has had their number circulated for many, many years, I can understand that. We cannot just begin to issue Social Security numbers just because someone has had their identity stolen.

But in the case of infants, which my two granddaughters—my son, one of the first things my son was told that he had to do when the grandbabies were born was, "You have to go get a Social Security card, and you have to have a Social Security number"—when I tried to open a savings account for them to start putting some money in there for their college education, I had to have a Social Security number. I mean I had to do this. So, he didn't feel like, as a parent, he had the option of not having a Social Security number.

And so, I am looking forward to the hearing today. Thank you for doing it. I am very interested in learning more about the Master Death File. With the amount of fraud going on in the country today, I mean the amount of fraud going on in this system, and with trillion-dollar deficits, I, as a Congressman, feel like I owe it to my constituents and the American public to make sure that we are good stewards of Social Security.

Chairman JOHNSON. Yes, thank you for your comments.

Mr. MARCHANT. Thank you.

Chairman JOHNSON. We have two panels today. And seated at the table is our first panel, and the only witness in the first panel, Commissioner of Social Security Michael J. Astrue. Welcome, Commissioner. You may proceed with your comments.

STATEMENT OF HON. MICHAEL J. ASTRUE, COMMISSIONER, SOCIAL SECURITY ADMINISTRATION

Mr. ASTRUE. Thank you, Mr. Chairman. Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, thank you for this opportunity to testify about the Social Security Death Master File and identity theft. This hearing marks our first opportunity to express our views to Congress on this important subject, and I commend you for adding it to your agenda.

Identity theft is a plague on our Nation, and one that is spreading. A hacker successfully targeted me just a few weeks ago, and so I know the frustration, anger, anxiety, and sense of violation that comes with this crime.

The Federal Government must do all that we can to reduce this plague, and we certainly should not make it worse. As my written testimony explains in detail, unintended application of the Freedom of Information Act to data in the Death Master File has created a new opening for cyberthieves. This form of identity theft is fairly recent, but appears to be growing. Accordingly, we must move swiftly to shut this activity down. For that reason we support the principles of Chairman Johnson's bill H.R. 3475, which would strike a fair and better balance between transparency and respect for privacy.

I should note that the Office of Management and Budget has been leading a review of this issue by interested Federal agencies, and we expect to offer a few improvements clarifying the terms and conditions by which Federal agencies and certain private organiza-

tions would have access to these data. These suggestions, however, should not slow Congress from moving forward aggressively with this important initiative.

In addition, we acknowledge that this legislation does not remove the need for us, at the Social Security Administration, to maintain the most accurate records possible.

Again, I commend the Committee for holding this hearing, and I would be happy to answer any questions you may have.

[The prepared statement of Mr. Astrue follows:]

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

HEARING BEFORE
COMMITTEE ON WAYS AND MEANS.
SUBCOMMITTEE ON SOCIAL SECURITY,
U.S. HOUSE OF REPRESENTATIVES

SOCIAL SECURITY AND DEATH INFORMATION

FEBRUARY 2, 2012

STATEMENT OF

MICHAEL J. ASTRUE
COMMISSIONER OF SOCIAL SECURITY

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee:

Thank you for inviting me to discuss the Social Security Administration's (SSA) Death Master File (DMF) and some of the known concerns. This hearing marks our first opportunity to express our views to Congress on this important subject, and I commend you for adding it to your agenda.

How We Use Death Information

We do not generate death data; rather, we collect it from a variety of sources so that we can run our programs. We receive about 2.5 million reports of death each year primarily from family members, funeral homes, financial institutions, and States. When we receive information about an individual, we update our records, including the Numident file,[1] which allows us to stop payment of benefits to a deceased beneficiary and establish benefits for survivors.

Experience shows that some sources, including family members and funeral homes, are highly accurate and we use them to administer our programs without further development. For other reports, such as those we receive from a non-family member, we verify the report if we need to use the death record to administer our programs. If the deceased person is not a beneficiary and no survivor benefits are payable, we do not verify the death report. However, we update the Numident with the death information.

Creation of the DMF

Individuals and entities became aware of the death information we gathered to run our programs. In 1978, Ronald Perholtz filed a lawsuit against us under the Freedom of Information Act (FOIA) to gain access to this information. Deceased individuals generally do not have privacy rights; therefore, after consulting with the Department of Justice, we settled the case by agreeing to disclose certain information about deceased individuals to Mr. Perholtz.

As legally mandated FOIA responses for death information increased, we decided in 1980 that the most efficient way to handle the growing requests was to create a file that we could make available to the public. That file is commonly known as the Death Master File, or DMF. Since 1992, we have provided the file to the Department of Commerce's National Technical Information Service (NTIS) to distribute because NTIS functions as a national clearinghouse for a wide array of Government data. NTIS reimburses us for the file under a contractual arrangement and then sells it to over 450 entities including banks, hospitals, universities, insurance companies, and genealogical services. In addition, NTIS makes the file available for online searching by many organizations with similar requirements but who do not wish to load the raw data on their internal systems. The financial services community in particular expressed a desire for this ability when the Subcommittee and the Financial Services Subcommittee on Investigations and Oversight held a joint hearing on the DMF in November 2001.

[1] The Numident contains identifying information associated with a Social Security Number, including a death indicator and parents' names.

Additional Statutory Requirements on Death Information

In 1983, Congress added subsection (r) to section 205 of the Social Security Act. This subsection requires us to collect death information from States to update our program records, provides the circumstances under which certain agencies may receive such information from us, and exempts the death information we receive from States from FOIA and the Privacy Act.

Pursuant to section 205(r), we provide Federal benefit-paying agencies with all of the death information in our records on a regular basis, including the death information we receive from the States. We provide an electronic file with all of our death records to the Centers for Medicare & Medicaid, Department of Defense, Government Accountability Office, Internal Revenue Service (IRS), Office of Personnel Management, Railroad Retirement Board, Department of Veterans Affairs, and Pension Benefit Guaranty Corporation. Federal benefit-paying agencies need death information to ensure accuracy of their benefit payments and prevent fraud, waste, and abuse. In addition, IRS has a complete copy of our Numident file, and we send them weekly updates.

Electronic Death Registration

As explained, we need accurate death information to properly administer our programs. Since 2002, we have worked with States and other jurisdictions to increase the use of Electronic Death Registration (EDR). EDR automates our receipt of death information and is highly accurate because the States verify the name and Social Security Number of deceased individuals against our records before they transmit the death report to us. Currently 32 states, the City of New York, and the District of Columbia participate in EDR.

Our death information is becoming even more accurate as more States participate in EDR. We realize, however, that a low error rate is meaningless to the living people whose information is erroneously divulged. We encourage States to participate in EDR to ensure our death records are as accurate as possible.

Possible Changes to the DMF

Identity theft is a spreading plague on our Nation. The Federal government must do all that we can to curtail this problem, and we certainly should not make it worse. Unfortunately, public access to the DMF has created opportunities for criminals. The media has reported incidents involving the use of death data to commit tax fraud. The most efficient way to help curtail fraud is by ensuring it is not released to those entities or individuals who might misuse it.

Without your support, any change we make to our procedures for disclosing information will be met with resistance, especially given our obligations under FOIA. For example, we recently removed the ZIP code and quickly received a FOIA request for that information. Trying to keep up with individual FOIA requests for information on millions of deceased individuals is a resource issue at a time when the agency is struggling to keep up with rising demand for services in a time of dwindling resources.

We support the basic principles of striking the balance between transparency and protecting individuals from identity theft that underlies Chairman Johnson's bill, H.R. 3475 "Keeping IDs Safe," and look forward to working with Congress, the Administration, and other parties on legislation that achieves that purpose.[2] The bill would continue to permit the disclosure of our death information, as under current law, to Federal benefit-paying agencies. We are currently part of an interagency group reviewing legislative options in this area, and may have some further suggestions that address the legitimate needs of a broad spectrum of organizations, including means by which outside parties with reasons to use the DMF might do so. We look forward to working with Congress to strike the proper balance between preventing fraud and abuse, and protecting individuals from identify theft.

Conclusion

We appreciate Congress' interest in working with us to protect our fellow Americans. We are committed to continuing to share death information with our Federal partners and appreciate that there are other parties that, with vigilant oversight, have reasonable and responsible purposes for obtaining death data. Under the provisions in subsection 205(r), the amount of publicly available data we share would continue to shrink if participation in EDR increases. We hope Congress will move quickly to address this problem.

I would be happy to answer any questions you may have.

[2] All statutes enacted after October 28, 2009, must also cite to 5 U.S.C. 552(b)(3) in order to withhold information from the public.

Chairman JOHNSON. As is customary for each round of questions, I will limit my time to 5 minutes and ask my colleagues to also limit their questioning to 5 minutes.

Commissioner, in your testimony you talk about your obligations under the Freedom of Information Act. And I am glad you did. In past audit reports, the Social Security Inspector General has criticized the agency for putting personal information of the deceased on the Death Master File, that the court settlement really did not require, according to him.

For example, you list a person's date of birth, the zip code, and the settlement did not require that information to be made public. You said you recently tried to do one simple thing, remove the zip code from the Death Master File, and you are already getting picked to death—excuse the pun—by inquiries and lawyers. Lawyers are going to pick you apart, regardless.

Fixing the death data system to protect both the living and dead from identity theft, and to allow the agency to go on with its important business, is Congress's responsibility, in my view. Isn't eliminating the publication of the Death Master File, as I propose, the best way to make sure none of this information about deceased is made public?

Mr. ASTRUE. Absolutely, Mr. Chairman. There has been some confusion. I think some of it has been fostered in the press. I think that some of the auditors, with all due respect for the Inspector General, are confused on this point.

The Perholtz Settlement in 1980, is based on the view that the Department of Justice came to in that litigation, that basically we had no choice, that we had to turn over the specific items requested in that litigation, so we entered into a consent decree.

The same rationale applies to other information. The legal analysis is exactly the same. So the fact that the settlement agreement does not specifically address certain data elements really isn't relevant at all, nor does Mr. Perholtz, as some irresponsible reporters have suggested, have the authority to dictate this to the Federal Government.

You are exactly right. Congress has said in the Freedom of Information Act, "You must release data of certain profile, unless Congress has provided you with an exception." Congress had not done that in 1980, hasn't done it now, and quite understandably, because it was not a problem back in that time period. But to your credit, Mr. Chairman, and to the credit of other Members of Congress, you have seen that the world has changed, you know that it is a problem now, and you know that we need action. And we support all that, and we want to support you in that action.

Chairman JOHNSON. Thank you, sir. You know, information is almost instant today. And if you put the wrong stuff out there, you are in trouble.

Mr. ASTRUE. That is for sure.

Chairman JOHNSON. Social Security has also been criticized by the Inspector General for putting individuals on the Death Master File who are not dead; 20,000 people over a 3-year period ending in April 2007, to be exact, according to one of their audits.

Your agency estimates the number to be about 14,000 per year. Countless news reports tell the horrifying stories of the personal

and financial hardship these people endure when these terrible mistakes are made. Isn't eliminating the Death Master File the only certain way to prevent these errors and potential ID thefts from occurring?

Mr. ASTRUE. Yes, it is, Mr. Chairman. And again, we have a remarkably accurate system overall, and we strive to make it more accurate. But it is a voluntary system. In some ways it is remarkable that we do as well as we do. No matter how we improve our own internal processes, we are not going to be able to eliminate all mistakes.

And potentially, the cost of those mistakes could be substantial. I think, up to this point, the living have been fortunate in that the big problems have been with the theft of identities from people who have, in fact, passed away.

But it is a horrible thing that people go through. And I have seen it. In one week, one of my closest relatives and one of my closest friends and neighbors were declared dead, one by our agency and one by one of our other Federal agencies. So I was right in the middle—it is a horrible thing to go through, and I understand that. We need to reduce that, irrespective of what we do on the Death Master File.

But you are absolutely right. The only way to make sure that when we make a mistake it doesn't have devastating public consequences, is to enact legislation that keeps the Death Master File more confidential than it is today.

Chairman JOHNSON. Yes. The Inspector General also found that Social Security's policy is not to inform Americans when they are victims of these kind of errors. Why can't you tell the victims, and let them take immediate action to protect themselves?

Mr. ASTRUE. Mr. Chairman, we are relooking at this now. We have been complying with OMB guidance in this area. We contract for monitoring of the credit of individuals who have had a brief exposure in the public. Then we notify them if there was any indication that there had been any irregularity in their credit or their finances.

But we are relooking at that now. Hopefully, it will be irrelevant very soon, because some version of your bill will be enacted by Congress this year.

Chairman JOHNSON. Thank you. Mr. Becerra has arrived. Do you want to question?

Mr. BECERRA. Of course, Mr. Chairman. And I want to apologize for being detained, because this is one of those hearings where I think we actually can get some things done pretty quickly, because there is strong bipartisan support, we have demonstrated that in the past. And so my apologies. It is an important hearing.

Chairman JOHNSON. You mean you agree with me?

Mr. BECERRA. Absolutely, Mr. Chairman. Absolutely. And that is on the record.

[Laughter.]

And Commissioner, it is great to see you here.

Mr. ASTRUE. Thank you.

Mr. BECERRA. And thank you very much. I know that you have been trying to tackle this, as well. I think every Member who sits on this Subcommittee has heard the stories. And I know we are

going to hear a pretty devastating story from one of our witnesses. So I think it is one of those things that we have to tackle.

Obviously, the issue is making sure we provide information out there to our government agencies and to the private sector entities that deal with personal data, so that they can make sure they have the tools to detect and prevent fraudulent use of personal information. But clearly, too much of the information is getting out to those who use it for the wrong reasons.

And so, Mr. Chairman, rather than go into any opening statement, if I could just ask for unanimous consent to enter my written statement into the record, I will go straight to some questions.

Chairman JOHNSON. Without objection, so ordered.

[The prepared statement of Hon. Xavier Becerra follows:]

Opening Statement
The Honorable Xavier Becerra, Ranking Member
Subcommittee on Social Security
February 3, 2012

Thank you, Mr. Chairman, for convening this hearing.

This Subcommittee has long been concerned about the problem of identity theft, where all too often it is the Social Security number which provides the key to committing the crime. For many years, we have worked on a bipartisan basis to examine and address identity theft. And, in a prior Congress, our Committee unanimously approved bi-partisan legislation designed to reign in the overuse of the Social Security number and to place limits on its widespread availability.

But today's hearing, I believe, will be one of our most compelling on this topic. In a few moments, we will hear from Jonathan Agin, who just last year lost his young daughter to a terrible cancer – and then was dealt another blow when his child's identity was stolen and used fraudulently to collect a tax refund.

No one should have to endure both the loss of a loved one and then the discovery that a heartless criminal has appropriated the deceased person's identity.

In the future, Mr. Chairman, I hope we can join with our colleagues on the Oversight Subcommittee to address the interrelated issues of identity theft and the administration of our tax laws, the latter of which is not within the jurisdiction of this Subcommittee.

Today's hearing will examine the use and availability of the so-called Death Master File, which is compiled by the Social Security Administration from the death records SSA obtains for the purpose of administering Social Security and SSI benefits. The File is made available for sale by the Department of Commerce to other public and private entities.

The reason this personal information is available for sale is because our nation's privacy protection laws, it turns out, only apply to living persons. In most cases, there are no protections for the identities and personal information of individuals who are deceased. As a result, SSA was compelled to make the Death Master File publicly available as a result of litigation in the late 1970s.

The data compiled in the File goes a long way in helping government agencies and private insurers, for example, to administer benefits, making sure that benefits do not continue after an individual's death. The File can also be used to detect and prevent fraud involving the identities of deceased persons. At the same time, that personal data is obviously getting into the wrong hands, too.

I know this Committee is committed to solving the problems surrounding the Death Master File. We need to keep the personal data of Americans -- living and deceased -- out of the hands of identity thieves. And, we should make sure there is a swift and stiff price to be paid for the transgression. Yet, somehow, fraud prevention tools must remain available to those who need them.

The challenge for this Subcommittee is crafting a solution that achieves that balance. I look forward to hearing from our witnesses about the extent of the problem, the challenges of shutting down fraud involving the identity of deceased persons, and possible solutions.

Mr. BECERRA. Thank you, Mr. Chairman. Commissioner, I guess the troubling aspect of this is that trying to find that balance in giving the information to those who need it so they can start to check records to make sure people aren't filing false applications for credit cards and so forth, and of course figuring out a way to make sure that that information stays tightly in the hands of those who need it. Is SSA looking at the possibility of trying to limit access to the records of deceased individuals?

Because my understanding is today the Master File essentially is sold once you have packaged it, once Commerce goes out there to sell it, they sell it to anyone who is willing to pay for it.

Mr. ASTRUE. Right. I am not speaking for the agency now, I am speaking on behalf of the Administration. As I mentioned in my remarks, we have a group that OMB has been leading for a while working on this issue. We have a lot of interested agencies.

So, we think the general principle—that the starting point is that instead of assuming that everything should be disclosed unless there is an exception, we should be moving the other way, with the presumption that information is withheld unless there are very specific rules as to who should get it, and what should be the protections and conditions that are built in to those arrangements.

Also, within the Federal Government, there is a little bit of a gap in the statute that I know has frustrated the President. The President is very interested in what used to be called the Do Not Pay List, which is now called GOVerify, and has directed everyone in the executive branch who is participating in that to use the Death Master File for program integrity purposes.

Unfortunately, the statute does not permit all the agencies that could benefit from program integrity efforts with the Death Master File to use those records, because right now we are only allowed to share with the benefit-paying agencies. We can, on a discretionary basis, share the Death Master File for research. But there is an area—I think very legitimate Federal use—where we can improve the operations of government significantly if we also have clearer and broader authority to share death information within the Federal agencies.

Mr. BECERRA. Do you think there is—can you answer this question? Is there a problem with the disclosure of the Death Master File to Federal agencies? Is there any evidence that it has been misused or loosely guarded by the agencies, so that we would have to put constraints on Federal agencies?

Mr. ASTRUE. I am not aware of any. From everything I know——

Mr. BECERRA. So it is mostly the fact that——

Mr. ASTRUE [continuing]. All Federal agencies have been careful in this regard. On the other hand——

Mr. BECERRA. So, let me ask this——

Mr. ASTRUE [continuing]. It would be appropriate to consider that.

Mr. BECERRA. Right. So we may want to take a look at what we need to do to safeguard it when other Federal agencies get the information.

Mr. ASTRUE. Right.

Mr. BECERRA. And making sure that they safeguard it as much as necessary as they use it.

This issue of outside entities getting to purchase, that is where we really have to be careful, because there is less control over that. Is there something that we can do quickly, where if it is, as you indicate there seems to be general agreement within the Federal Government, that we have to try to figure out a way to not give it out, this information out, so quickly.

Is there something that we can act on bipartisanly quickly so that we can not just send messages that we want to try to safeguard the information, but that we can actually get underway with something that actually requires those that obtain this information to keep it secure? And, quite honestly, punishes those who misuse the information?

Mr. ASTRUE. Right. So—and I am not trying to be cute here—it depends a little bit on your definition of "quickly." I know from participating in this interagency group, which has been working hard, that this is a lot more difficult than it looks at first. And if you do it quickly, as in a month, 6 weeks, the chances are pretty high that you will get it wrong, because there are hard and important balances here.

Mr. BECERRA. I agree with that.

Mr. ASTRUE. And this needs to be crafted extremely carefully.

On the other hand, if you are defining "quickly" as can we get it passed this year, my answer to that would be yes, we have to go pedal to the metal, work in a way between the Houses, between the parties, between the Congress and the executive branch, that doesn't happen very often these days. But I think that we can do it, because I have talked to a lot of Members, both Houses, both parties. I don't think this is one of those issues where you are badly divided.

Mr. BECERRA. I agree.

Mr. ASTRUE. I think this is largely working out the technical issues. So I think that if we can focus, we get help, get the spirit, work openly with the group at OMB, I think that we can get this done. I think it probably will take a couple months to work through all the details and craft the actual language that draws these difficult balances the right way. But I think it is doable in a few months.

Mr. BECERRA. Mr. Chairman, maybe one thing we can really concentrate on is working with the Commissioner and whatever agencies are appropriate to have at the table and see if we can—I wouldn't want to rush it, either. I know you wouldn't want to rush it, either. But to the degree that there might be a chance, I think we should explore that.

Chairman JOHNSON. Yes, I agree. And I mentioned earlier, before you got here, that we are going to have a joint hearing with another Committee to try to see if we can't figure something out.

Mr. BECERRA. Excellent, excellent.

Chairman JOHNSON. It is a continuous problem that can't be solved right now, but needs to be addressed, certainly.

Mr. ASTRUE. And I want to say I will do everything I know how to do to do this. I want to commend OMB, because I think Martha

Coven and Shelley Metzenbaum have done a great job trying to get agencies with very different perspectives to work on this issue.

I had been hopeful that maybe I could come up with more specificity today. But I think it is more important to get it right than to get it fast.

Mr. BECERRA. Yes, yes.

Mr. ASTRUE. So I would encourage you, as you figure out the best way to work on it with your staffs, to also reach out directly to the folks at OMB who I think are doing a——

Mr. BECERRA. And let us know——

Chairman JOHNSON. You need to work on your guys down there and make sure they don't make injuring errors any more.

Mr. BECERRA. And, Mr. Chairman, let us—Mr. Commissioner, you should let us know if we can help you excite some of the other agencies to participate. And while they may be very busy, they may not be as enthusiastic or animated in moving this quickly. And let us know if we can help you animate them.

Mr. ASTRUE. I think——

Chairman JOHNSON. Well, this is one of those issues that——

Mr. ASTRUE. I think there are occasions, Mr. Becerra, where we do appreciate that help. I think in this particular case it is fair to say that in the beginning it took a little while because it is a new issue, and I think we have the agencies, whose attention needs to be focused on this, very focused on it.

Chairman JOHNSON. Yes.

Mr. ASTRUE. And in fact, we have had very animated discussions about this. It is going to take us another month or so, probably, to give you the more detailed feedback that you probably need to go forward.

Mr. BECERRA. Great. Thank you.

Chairman JOHNSON. Thank you. And, Mr. Marchant, do you care to question?

Mr. MARCHANT. I have one question. A constituent has contacted me recently, and this constituent is heavily into research of her ancestry. And I suspect that there are millions like her. How can we be careful in what we do to make sure that the people that are harmed are protected, but those people that are vitally interested in their ancestry can still access accurate information?

Mr. ASTRUE. I know that there is concern with the genealogists. I think that raises some challenges that we don't have when we are talking about large institutions that can be fined and penalized easily by the Federal Government if there is inappropriate use.

I do think that in most cases, genealogists can find the information that they really want from other sources. I have seen some of the communications from those groups, and I do think it is an overreaction right now.

I think that probably what we need to do is to talk about a different framework, in terms of perhaps eventual release. That is what happens with Census data.

But I honestly am not persuaded that, in the short run, withholding it for some period of years is going to seriously impair genealogical research, which I have done myself. I have been working on a project in my own family. So I appreciate the dedication that people have to it. But at some point I think what comes first

has to be families that have four-year-olds whose identity is stolen, and those types of things. I think that is what comes first.

And then I think the question is, is there a way, or what is the best way, to accommodate those other interests, and does that mean a delay in release for some extended period of time? Whether that is 10 years, whether that is 75 years, like the Census. Those are questions that we have talked about in the interagency group, but we have not come to resolution on those or a lot of the related issues yet, because they are hard issues.

Mr. MARCHANT. Thank you. Thank you, Mr. Chairman.

Chairman JOHNSON. Let me just ask a question that kind of follows up on what he said. When are we going to receive your recommendations to address this problem?

Mr. ASTRUE. I would hope, Mr. Chairman, that it would be piecemeal in real time. I think that as many of these conversations that we can have as quickly as possible would be the best.

I think there are certain ones that are fairly easy. If you go back and look at the congressional hearings in the wake of 9/11, Congress had a lot of interest in us getting more, better Death Master File data out faster to the financial communities to try to prevent money laundering and the kinds of things that can fund terrorism.

There are court orders right now requiring life insurance companies to use the Death Master File so that they pay insurance claims that are due, and don't use the fact that some claims are not pursued as a way of just making more money. So there is a bunch of issues.

I think the financial corporations are probably the easiest. I think we have had a fair amount of usage from educational and health care institutions. I think those are probably fairly easy. I think questions like the genealogists are much trickier and will take some time.

So what I would say is I would hope that we would be talking substantially more guidance on some issues within a matter of weeks. But maybe not everything, because we have a lot of agencies that, quite candidly, right now, have a different perspective on some of these issues. So I can't come up and speak to you authoritatively until we coordinate agreement on that. In some issues that should be very soon, in some it will probably take a little bit longer.

Chairman JOHNSON. Okay. Well, let's work together and try to get it done as quickly as we can.

Social Security, in the past, has provided funds to the National Association for Public Health Statistics and Information Systems to develop and implement the electronic verification of vital events. This is an online system that verifies birth and death information through a single interface. Does this system have the potential, in your view, to be the go-to agency for the death information now provided by the Death Master File?

Mr. ASTRUE. We will certainly take a look at that, Mr. Johnson. I think it has been difficult enough getting a database the way that we are doing it now. I would be a little bit reluctant to start over. But I will certainly look into this. It is a question that just came to my attention recently. I was not terribly aware of this. So we will look at that in good faith.

What I will say also, regarding funding to support our electronic death registration, authority moved over to HHS on that, and there has not been money appropriated to accelerate that process. We have, I believe, 32 States and 2 jurisdictions that are at least partially participating in that system. The relatively small amount of money to get the other 18 States on board, I think, would do a lot to make the system more accurate, faster, and better for everybody that is using it.

[The statement of Mr. Astrue #1 follows:]

Table of Contents

Section A - Standard Form 1449 (SF 1449)

Section B -- Addendum to Standard Form 1449

In accordance with Federal Acquisition Regulation (FAR) 12.302 and 12.303, this addendum to the Standard Form (SF) 1449 provides for continuation of the schedule and description of the supplies/services to be acquired.

B-1 PRICE/COST TABLES

The contractor shall provide the designated jurisdiction's vital statistic death record data by electronic transmission methods which conform to SSA's requirements and format. This information shall be provided for the contract period (Calendar Year [CY] 2012 through 2016). The data shall be in the format prescribed in the attachment . Duplicate death data provided in the same or subsequent transmissions shall be paid for only once.

NOTE: For purposes of this contract, a jurisdiction has transitioned to the Electronic Death Registration (EDR) process when it has incorporated SSA's Online Verification Software into its Electronic Death Registration System AND has submitted to SSA one live death record with a verified SSN.

States may exercise the right to transition from the Non-EDR process to the EDR process during the course of the contract period. If states exercise this option, they will receive one payment for "processed records"[1] submitted timely in the applicable format. If states transition, they are not entitled to both Non-EDR and EDR payment rates for the same death records.

States will be paid the full unit price (see chart below) for processed records (Non-EDR or EDR) submitted within 120 business days after the date of death. States will only be entitled to $.01 for records submitted 121 days or more beyond the date of death. The records submitted after 120 days will be present on the death process notices in May 2012 and will be effective on invoices starting in the 2nd quarter of CY2012 (April-June 2012).

The following payment schedule shall be in accordance with the receipt of Electronic Death Registration (EDR) records (verified and unverified) and Non-EDR records:

Base Year: January 2012 – December 2012	**Quantity Estimated**	**Unit**	**Unit Price**	**Total**
EDR Receipt of Records: Within 6 Business Days of Death		Record	$2.86	
EDR Receipt of Records: Between 7-30 Business Days of Death		Record	$1.43	
EDR Receipt of Records: Between 31-120 Business Days of Death		Record	$0.80	
Receipt of Records: Non-EDR Submitted Within 120 Business Days of Death		Record	$0.80	
Receipt of Records (Both Non-EDR and EDR (added in May 2012): Beyond 120 Business Days of Death		Record	$.01	
Total Estimated Quantity				

Addendum to SF-1449
Electronic Death Records for SSA

Option Year I : January 2013-December 2013	Quantity Estimated	Unit	Unit Price	Total
EDR Receipt of Records: Within 6 Business Days of Death		Record	$2.93	
EDR Receipt of Records: Between 7-30 Business Days of Death		Record	$1.47	
EDR Receipt of Records: Between 31-120 Business Days of Death		Record	$0.82	
Receipt of Records: Non-EDR Submitted Within 120 Business Days of Death		Record	$0.82	
Receipt of Records (Both Non-EDR and EDR): Beyond 120 Business Days of Death		Record	$.01	
Total Estimated Quantity				

Option Year II: January 2014-December 2014	Quantity Estimated	Unit	Unit Price	Total
EDR Receipt of Records: Within 6 Business Days of Death		Record	$3.01	
EDR Receipt of Records: Between 7-30 Business Days of Death		Record	$1.51	
EDR Receipt of Records: Between 31-120 Business Days of Death		Record	$0.84	
Receipt of Records: Non-EDR Submitted Within 120 Business Days of Death		Record	$0.84	
Receipt of Records (Both Non-EDR and EDR): Beyond 120 Business Days of Death		Record	$.01	
Total Estimated Quantity				

Option Year III: January 2015-December 2015	Quantity Estimated	Unit	Unit Price	Total
EDR Receipt of Records: Within 6 Business Days of Death		Record	$3.09	
EDR Receipt of Records: Between 7-30 Business Days of Death		Record	$1.55	
EDR Receipt of Records: Between 31-120 Business Days of Death		Record	$0.86	
Receipt of Records: Non-EDR Submitted Within 120 Business Days of Death		Record	$0.86	
Receipt of Records (Both Non-EDR and EDR): Beyond 120 Business Days of Death		Record	$.01	
Total Estimated Quantity				

Option Year IV: January 2016 - December 2016	Quantity Estimated	Unit	Unit Price	Total

EDR Receipt of Records: Within 6 Business Days of Death		Record	$3.17	
EDR Receipt of Records: Between 7-30 Business Days of Death		Record	$1.59	
EDR Receipt of Records: Between 31-120 Business Days of Death		Record	$0.88	
Receipt of Records: Non-EDR Submitted Within 120 Business Days of Death		Record	$0.88	
Receipt of Records (Both Non-EDR and EDR): Beyond 120 Business Days of Death		Record	$.01	
Total Estimated Quantity				

The rate per record will increase annually by 2.28%, which represents the average Consumer Price Index (CPI) percentage increase for the previous five-year period (2007-2011).

[1]Processed Record: Death record data transmitted to Social Security Administration within the timeframes established in Section B-1. This does not include duplicated records.

SECTION B-2 DESCRIPTION/SPECIFICATIONS/ STATEMENT OF WORK

B-2.1 BACKGROUND

As required by Section 205(r) of the Social Security Act, the Commissioner of the Social Security Administration (SSA) is directed to seek voluntary cooperation of the States in providing death record information under contractual agreements for use in the administration of the programs established under the Social Security Act, as amended. SSA shall carry out this provision of the law. The purpose of this program is to reduce erroneous payments to deceased persons receiving Social Security benefits.

B-2.2 SCOPE OF WORK

The contractor shall furnish the necessary personnel, materials, services, facilities and equipment, except as may otherwise be specified herein, and perform all tasks necessary for, or incidental to, the performance of the work set forth herein.

The contractor shall provide vital statistic death record data by electronic transmission methods which conform to SSA's requirements and format. The death data shall be provided beginning approximately January 1, 2012 through December 31, 2016. The data shall be transmitted in the Format prescribed in the attachment.

Electronic Death Registration (EDR) Records

EDR Records are death reports that go through an online SSN verification check prior to submission to SSA. EDR records that pass the online SSN verification are referred to as "verified EDR" records. EDR records that do not pass the online SSN verification are referred to as "unverified EDR" records.

The contractor shall provide EDR records to SSA within six business days from the date of death in order to receive full payment. Saturdays, Sundays, and Federal Holidays will not be used in the calculation of the six

business days. For EDR records submitted seven business days or more beyond the date of death, SSA will reimburse the contractor at a lower rate.

Funeral homes, hospitals, coroners, etc., will initially verify these EDR records by accessing the online SSN verification system through a State/Jurisdiction EDR system. If there is a data match, SSA shall begin the termination process for the deceased beneficiary once it receives the Verified EDR record from the State/Jurisdiction Vital Records.

No Verification Attempt EDR Records

No Verification Attempt EDR Records are electronic death records that do not go through the online SSN verification process because they are missing mandatory fields (See Attachment A) or because the jurisdiction does not have the online SSN verification process integrated with their EDR system. For SSA purposes, No Verification Attempt EDR Records will be included in the Non-EDR record counts on the Death Process Notice.

Non-EDR Records

Non-EDR records are death reports that do not go through an online SSN verification check prior to submission to SSA.

There may be some situations when the contractor can only provide Non-EDR death records. The contractor shall submit these records at least once each month. This death data is generally recorded within 90 days of occurrence. Therefore, Non-EDR deaths occurring between the first and last day of a month shall be included in the transmission submitted on or before the last day of the month following the 90-day period. For example, deaths occurring 01/01/12 through 01/31/12 shall be included in the transmission due to SSA on or before the last day of April 2012.

Death Record Submission Requirements
All death records submitted to SSA should reflect at least a first name and a last name. Middle names should be included where available. The State/Jurisdiction shall submit to SSA the name of the decedent as they receive it, within the field limits specified by SSA. The State/Jurisdiction shall not submit decedents whose name is unknown, nor should "John Doe's" or "Jane Doe's" be submitted. See the attachment for the State Death Record Format.

The record files are transmitted to the National Computer Center, Baltimore, Maryland. The contractor shall advise the Contracting Officer's Technical Representative (COTR) and the Contracting Officer (CO) of any change made to the contractor's internal system(s), which may impact the data transmitted to SSA. Such notice must be made at least 7 days in advance of transmission of data which may be affected by such a change. This requirement is necessary to avoid potential adverse effects to the SSA systems already in existence to process the contractor's data.

Invoices shall include information indicated in C-2 Invoice Submission and Payment Related Information.

Section C. Contract Clauses And Terms And Conditions

C-1 FAR Clause 52.212-4 Contract Terms and Conditions - Commercial Items (June 2010)

In accordance with FAR 12.301 and 12.302, the clause 52.212-4 is incorporated herein by reference via Block 27 of Standard Form (SF) 1449, Solicitation/Contract/Order for Commercial Items.

C-2 Addendum to FAR Clause 52.212-4, Contract Terms and Conditions – Commercial Items (June 2010)

- Paragraph (g), Invoice, is supplemented as follows:

Invoice Submission and Payment Related Information
The contractor will receive invoices, prepared by SSA, for review and verification via email or fax. The invoice will include all of the elements defined in the invoice or payment clause used in this award as well as any other information required below or in the contract.

Other Required Information:

The following information shall be included on all invoices: invoice number; contract number; and delivery order number (a new one is designated for each year of the contract.) In addition, the invoices shall include:
--Processing Date(s)
--Number of records transmitted for each processing date
--Number of records processed for each processing date
--Total number of processed records
--Rate of Payment
--Total payment amount requested
The year of performance is broken into four quarters:
Quarter 1: January, February, March
Quarter 2: April, May, June
Quarter 3: July, August, September
Quarter 4: October, November, December

Payment shall only be made for death records that SSA can process. In other words, the contractor will refer to the two SSA DEATH PROCESS NOTICES as reflected in Attachment D to determine the number of processed death records. SSA will pay for the number of records indicated under the heading of "PROCESSED" in the section "REPORT COUNTS BY YEAR". SSA will not pay for the number of error records that are included under the heading "EXCEPTED".

Using a direct payment system [2], SSA will send invoices to the contractor in April, July, October and January. The invoices will summarize the death record data transmitted and the proposed quarterly payment. The contractor shall review the invoices before payment is disbursed. After review and concurrence, the Contracting Officer's Technical Representative (COTR) will authorize the Division of Finance to make the final payment.

[2]Direct Payment System: A system by which invoices are created quarterly by SSA for each state based on the number of processed death records received.

IF THE CONTRACTOR AGREES WITH THE INVOICE:
Upon receipt of the invoice, if the state agrees that the information is correct, correspondence via email should be sent to DCO.OPSOS.DRMI.EDR@ssa.gov stating their concurrence.

IF THE CONTRACTOR DISAGREES WITH THE INVOICE:
Submit amended invoices via email to DCO.OPSOS.DRMI.EDR@ssa.gov or fax to (410)965-7497 ATTN: EDR/Non-EDR COTR. When sending amended invoices, please include your Taxpayer Identification Number (TIN), your Dun &Bradstreet Number (DUNS#), and the Order Number on each invoice.
If there are invoice discrepancies, payment will be determined by the receipt of processed records reflected in SSA's systems. Final invoices will be sent to:

INVOICE SUBMISSION AND PAYMENT RELATED INFORMATION (DEC 2011)

The invoice shall include all elements of a proper invoice as defined in the invoice or payment clause used in this award and any other information required below or in any other contract clause. To assist the Government in making timely payments, include the contractor's Taxpayers Identification Number, Data Universal Numbering System number, contract, and the Order Number, if any, on each invoice.

Facsimile (Fax) communication is the preferred method of submission for invoices and public vouchers, because the invoice will be received directly into the SSA payment system. If the invoice cannot be faxed, submit it electronically via email, by regular mail, or by hand carrying it to the Office of Finance at the address below.

If submitting by fax, use any one of the following fax numbers:

410 965-8209
410 965-8251
410 965-8200
410 965-8216
410 966-5425
410 966-9940
410 965-3734
410 965-7533

If submitting electronically:

Submit the invoice either as an attachment to an email message, or within the message itself, to: OTAPS.DAPS.Invoices@ssa.gov.

If sent by mail, submit an original and three (3) copies of the invoice to:

Social Security Administration
Office of Finance
Post Office Box 47
Baltimore, Maryland 21235-0047

If hand carried, deliver to:

Social Security Administration
Office of Finance
Customer Service Help Desk
2-B-4 East Low Rise Building

6401 Security Boulevard
Baltimore, Maryland 21235-0047

The telephone number of the finance customer service help desk is (410) 965-0607.

The Government will make payment to the Contractor using the Electronic Funds Transfer (EFT) information contained in the Central Contractor Registration (CCR) database. In the event that the EFT information changes, the Contractor shall be responsible for providing the updated information to the CCR database. The EFT information submitted must be that of the contractor unless there is an official Assignment of Claims on file with the Office of Finance.

Remittance information associated with EFT payments is available via the Internet Payment Platform (IPP) on the Department of Treasury's Internet site at http://www.ipp.gov.

The Contractor may also direct payment inquiries to SSA's Office of Finance by:

- Using its Financial Interactive Voice Response System (FIVR). FIVR is an automated self-service telephone system available 24 hours a day that allows direct electronic access to administrative payment information using the telephone keypad. The contractor can access FIVR by calling (410) 965-0607. The services available through FIVR are available through a Telecommunications Device for the Deaf (TDD) Line at 410-597-1395. Customer Service Representatives will be available to answer vendor payment inquiries Monday - Friday, between 8 a.m. and 4:30 p.m., Eastern Time.

By sending an email to payment.inquiries@ssa.gov, or visiting the internet site at http://www.socialsecurity.gov/vendor/contact.htm. The contractor can also access the IPP system through a link on this site.

C-3 FAR Clause 52.212-5, CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (AUG 2011)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:
(1) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).
___Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).
(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Pub. L. 108-77, 108-78).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

_X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I
(Oct 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).
___ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)
__X_ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jul 2010) (Pub.
L. 109-282) (31 U.S.C. 6101 note) __N/A (5) 52.204-11, American Recovery and Reinvestment Act—Reporting Requirements (Jul 2010) (Pub.
L. 111-5).
__ (6) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Dec 2010) (31 U.S.C. 6101 note).
__ (7) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).
___ (8) 52.219-3, Notice of Total HUBZone Set-Aside or Sole-Source Award (Jan 2011) (15 U.S.C. 657a).
___ (9) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).
___ (10) [Reserved]
___ (11)(i) 52.219-6, Notice of Total Small Business Set-Aside (June 2003) (15 U.S.C. 644).
__ (ii) Alternate I (Oct 1995) of 52.219-6.
__ (iii) Alternate II (Mar 2004) of 52.219-6.
____ (12)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
__ (ii) Alternate I (Oct 1995) of 52.219-7.
__ (iii) Alternate II (Mar 2004) of 52.219-7.
____ (13) 52.219-8, Utilization of Small Business Concerns (Jan 2011) (15 U.S.C. 637(d)(2) and (3)).
___(14)(i) 52.219-9, Small Business Subcontracting Plan (Jan 2011) (15 U.S.C. 637(d)(4)).
__ (ii) Alternate I (Oct 2001) of 52.219-9.
__ (iii) Alternate II (Oct 2001) of 52.219-9.
__ (iv) Alternate III (Jul 2010) of 52.219-9.
____ (15) 52.219-14, Limitations on Subcontracting (Dec 1996) (15 U.S.C. 637(a)(14)).
____ (16) 52.219-16, Liquidated Damages—Subcon-tracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
____ (17)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).
__ (ii) Alternate I (June 2003) of 52.219-23.
____(18) 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting (Dec 2010) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).
____ (19) 52.219-26, Small Disadvantaged Business Participation Program—Incentive Subcontracting (Oct 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).
____(20) 52.219-27, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (May 2004) (15 U.S.C. 657 f).
_X_ (21) 52.219-28, Post Award Small Business Program Rerepresentation (Apr 2009) (15 U.S.C. 632(a)(2)).
__ (22) 52.219-29 Notice of Total Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Apr 2011).
__ (23) 52.219-30 Notice of Total Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Apr 2011).

__X (24) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
__X (25) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jul 2010) (E.O. 13126).
__X (26) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).
__X (27) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).
__X (28) 52.222-35, Equal Opportunity for Veterans (Sep 2010)(38 U.S.C. 4212).
__X (29) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).
__X (30) 52.222-37, Employment Reports on Veterans (SEP 2010) (38 U.S.C. 4212).
__ (31) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
__X (32) 52.222-54, Employment Eligibility Verification (JAN 2009). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
__ (33)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
__ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
____(34) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007) (42 U.S.C. 8259b).
____(35)(i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007) (E.O. 13423).
__ (ii) Alternate I (DEC 2007) of 52.223-16.
____ (36) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011) (E.O. 13513).
____ (37) 52.225-1, Buy American Act—Supplies (Feb 2009) (41 U.S.C. 10a-10d).
____ (38)(i) 52.225-3, Buy American Act—Free Trade Agreements—Israeli Trade Act (June 2009) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, Pub. L. 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, and 110-138).
__ (ii) Alternate I (Jan 2004) of 52.225-3.
__ (iii) Alternate II (Jan 2004) of 52.225-3.
_____(39) 52.225-5, Trade Agreements (AUG 2009) (19 U.S.C. 2501, *et seq*., 19 U.S.C. 3301 note).
_____(40) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
_____ (41) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
_____(42) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
_____(43) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).
_____(44) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).
__X (45) 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration (Oct 2003) (31 U.S.C. 3332).
____ (46) 52.232-34, Payment by Electronic Funds Transfer—Other than Central Contractor Registration (May 1999) (31 U.S.C. 3332).
_____(47) 52.232-36, Payment by Third Party (Feb 2010) (31 U.S.C. 3332).

_____(48) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
_____(49)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).
__ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate.*]

_____ (1) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, *et seq.*).
_____(2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989) (29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).
_____(3) 52.222-43, Fair Labor Standards Act and Service Contract Act—Price Adjustment (Multiple Year and Option Contracts) (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).
_____(4) 52.222-44, Fair Labor Standards Act and Service Contract Act—Price Adjustment (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).
_____ (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (Nov 2007) (41 351, *et seq.*).
_____(6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services—Requirements (Feb 2009) (41 U.S.C. 351, *et seq.*).
_____ (7) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Mar 2009) (Pub. L. 110-247).
_____(8) 52.237-11, Accepting and Dispensing of $1 Coin (Sept 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (Dec 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) [Reserved]

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (Sep 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, *et seq.*).

(ix) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).
___Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (Nov 2007) (41 U.S.C. 351, *et seq.*).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (Feb 2009) (41 U.S.C. 351, *et seq.*).

(xii) 52.222-54, Employment Eligibility Verification (JAN 2009).

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Mar 2009) (Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

C-4 Additional FAR Clauses Incorporated by Reference

52.252-2 Clauses Incorporated By Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also,

the full text of a clause may be accessed electronically at this address:
https://www.acquisition.gov/far/index.html

52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Sept 2006)

52.232-18 Availability of Funds (APR 1984)

C-5 Additional FAR Clauses Incorporated by Full Text

The following FAR clauses are hereby incorporated into this solicitation/ contract by full text as follows:

C-5.1 52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from

January 1, 2012 through December 31, 2012 for Year One (1)

January 1, 2013 through December 31, 2013 for Year Two (2)

January 1, 2014 through December 31, 2014 for Year Three (3)

January 1, 2015 through December 31, 2015 for Year Four (4)

January 1, 2016 through December 31, 2016 for Year Five (5)

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

C-5.2 52.216-19 Order Limitations (Oct 1995)

(a) *Minimum order*. When the Government requires supplies or services covered by this contract in an amount of less than 100 records, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order*. The Contractor is not obligated to honor-

(1) Any order for a single item in excess of the total estimated quantity as shown in Section B.1 for the applicable ordering period;
(2) Any order for a combination of items in excess of the total estimated quantity as shown in Section B.1 for the applicable ordering period; or
(3) A series of orders from the same ordering office within ten (10) days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within ten (10) days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

C-5.3 52.216-21 REQUIREMENTS (OCT 1995)

(a) This is a requirements contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies or services specified in the Schedule are estimates only and are not purchased by this contract. Except as this contract may otherwise provide, if the Government's requirements do not result in orders in the quantities described as "estimated" or "maximum" in the Schedule, that fact shall not constitute the basis for an equitable price adjustment.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. Subject to any limitations in the Order Limitations clause or elsewhere in this contract, the Contractor shall furnish to the Government all supplies or services specified in the Schedule and called for by orders issued in accordance with the Ordering clause. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(c) Except as this contract otherwise provides, the Government shall order from the Contractor all the supplies or services specified in the Schedule that are required to be purchased by the Government activity or activities specified in the Schedule.

(d) The Government is not required to purchase from the Contractor requirements in excess of any limit on total orders under this contract.

(e) If the Government urgently requires delivery of any quantity of an item before the earliest date that delivery may be specified under this contract, and if the Contractor will not accept an order providing for the accelerated delivery, the Government may acquire the urgently required goods or services from another source.

(f) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period.

C-5.4 52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months.

The Contracting Officer may exercise the option by written notice to the Contractor within ten (10) days prior to the expiration date of the contract.

C-5.5 52.217-9 Option to Extend the Term of the Contract.

Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

C-6 Additional Agency Specific Terms and Conditions

The following agency-specific terms and conditions are hereby incorporated into this solicitation/contract by full text as follows:

C-6.1 PERIOD OF PERFORMANCE

The period of performance under this contract shall be from 01/01/2012 through 12/31/2016. The total duration of this contract shall not extend beyond 60 months, broken down as follows:

C-6.1.1 Contract Year (1):
January 1, 2012 through December 31, 2012

C-6.1.2 Contract Year (2)
January 1, 2013 through December 31, 2013.

C-6.1.3 Contract Year (3)
January 1, 2014 through December 31, 2014.

C-6.1.4 Contract Year (4)
January 1, 2015 through December 31, 2015.

C-6.1.5 Contract Year (5)
January 1, 2016 through December 31, 2016.

C-6.2 DESIGNATION OF GOVERNMENT CONTRACT SPECIALIST

Deborah Lawrence-Wilson, Contract Specialist, Division of Operations Contracts, has been assigned to administer the contractual aspects of this contract. However, changes in the Scope of Work, contract cost, price, quantity, and quality or delivery schedule shall be made only by the Contracting Officer by a properly executed modification. All correspondence that in any way concerns the terms or conditions of this contract shall be submitted directly to the Contract Specialist at the following address:

Social Security Administration
Office of Acquisition and Grants
Attention: **Deborah Lawrence-Wilson**
Contract Specialist
1st Floor, Rear Entrance
7111 Security Boulevard
Baltimore, Maryland 21244
Telephone Number –410-965-9532
Facsimile Number –410-966-9310
Email: Deborah.Lawrence-Wilson@ssa.gov

C-6.3 CONTRACT ADMINISTRATION

The contractor's representative responsible for handling contract administration is:

NAME:	
TITLE:	*(to be completed at time of award)*
ADDRESS:	*(to be completed at time of award)*
PHONE:	*(to be completed at time of award)*
FAX:	*(to be completed at time of award)*
EMAIL:	*(to be completed at time of award)*

C-6.5 DESIGNATION OF GOVERNMENT CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

(a) The individual(s) named below is hereby designated as the Government Contracting Officer's Technical Representative (COTR). If an Alternate COTR is also listed below, that person will serve in the COTR's stead when the COTR is unavailable. The COTR is responsible for the technical administration of this contract.

NAME: Kate Nagel	Alternate COTR NAME: Hellen Savoy
ADDRESS: 6401 Security Blvd 4230 Anx Baltimore, MD 21235	ADDRESS: 6401 Security Blvd 4243 Anx Baltimore, MD 21235
PHONE: (410) 965-8444	PHONE: (410) 965-9976
FAX: (410) 965-7497	FAX: (410) 965-7497
EMAIL: Kate.Nagel@ssa.gov	EMAIL: Hellen.I.Savoy@ssa.gov

(b) The COTR, or his/her authorized representative, shall be responsible for coordinating with the contractor the technical aspects of the contract. The COTR is not authorized to make any changes which affect the contract amount, terms or conditions. The Contracting Officer is the only person with the authority to act as agent of the Government under this contract. Only the Contracting Officer has authority to: (1) direct or negotiate any changes in the Statement of Work; (2) modify or extend the period of performance; (3) change the delivery schedule; (4) authorize reimbursement to the contractor any costs incurred during the performance of this contract; or (5) otherwise change any terms and conditions of this contract.

C-6.6 LIMITATION ON USE AND DISCLOSURE OF STATE RECORDS

LIMITATION ON USE AND DISCLOSURE OF STATE RECORDS

General
(a.) SSA recognizes that State laws governing the collection, use, and dissemination of death records may affect the conditions under which such records are made available to SSA. Therefore, SSA shall adopt policies and procedures to ensure that information received from the State shall be used by SSA in accordance with Federal law, section 205(r) of the Social Security Act, and this contract.

(b.) The State vital statistics data shall remain the property of the State. Except as set forth in this contract, the State data shall not be shared or otherwise made available to any agency or individual outside SSA, and working copies (if any) shall be destroyed after they have been used to update SSA's files.

Use of State Records by SSA – Screening for Erroneous Benefit Payments
(c.) Except as provided in Federal law, section 205(r) of the Social Security Act, and this contract, data from the State's death files shall be used only to screen SSA's payment erroneously issued to beneficiaries after their deaths. These payment systems include benefit entitlement information for the retirement, survivors, disability and health insurance programs established under titles II and XVIII of the Social Security Act and contain information pertaining to individuals entitled to Supplemental Security Income and part B, Black Lung benefits, which are programs also administered by SSA. In performing this match, when a State record either contains insufficient information or matches a payment record but the individual's death was already reported to SSA (and the month and year agree), the State record shall be dropped from the match operation and destroyed.

Use of State Records by SSA – Independent Verification
(d.) When a benefit record match occurs and SSA was either previously unaware of the individual's death or the date of death reported to SSA differs materially from that indicated in the State provided record, SSA will complete an independent verification of the fact and date of death before taking any action that would affect the beneficiary's entitlement to monthly payments. Such independent verification shall, at a minimum, consist of an attempted contact with the beneficiary at his or her last known address to verify continuing entitlement to benefits. In making such attempted contacts, SSA will not, under any circumstances, disclose the fact that report of the beneficiary's death was received from the State. After SSA completes an independent verification of the State record, SSA will delete the State source code from the record. The State waives the independent verification requirement for any EDR record that SSA receives with a verified SSN.

Death Master File
(e.) The Death Master File (DMF) is an extract of the death information from SSA's Numident, the electronic database that contains SSA's records of every individual who has applied for and been assigned a SSN. The Numident contains death records SSA receives from the States and from sources other than the States, including but not limited to a decedent's family member. SSA will screen the State death reports to determine if the SSN listed for each report was issued, according to SSA's records, to the deceased person identified in the report. Death records with SSNs assigned to someone other than the deceased will be dropped from further processing and destroyed and will not be included in the DMF.

Recipients of SSA's Death Master File
(f.) SSA will only disclose state death information pursuant to Federal law and section 205(r) of the Social Security Act. In accordance with section 205(r) of the Social Security Act, SSA must, provide

Federal Benefit paying agencies with a complete copy of SSA's DMF. Federal and State agencies receiving death records will be required under the terms of its contract with SSA to use the information only for the agreed upon purpose and to independently verify the fact and date of death of an individual before taking any action affecting such person's entitlement to benefits.

The Public Death Master File shall not contain any information where the source of information is State Vital Records' offices.

Records NOT Independently Verified by SSA
(g.) In accordance with section 205(r) of the Social Security Act, supplied State death data that is unverified under terms of this contract is exempt from disclosure under the Federal Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). SSA will remove all State death data that are unverified from the Public Death Master File.

EDR Records with a Verified SSN by SSA
(h.) SSA will immediately and automatically terminate benefits for any beneficiary whose death record is submitted to SSA through the State's EDRs, provided that the death record contains a verified SSN.

C-6.7 SAFEGUARDS

The Social Security Administration agrees to the following conditions regarding safeguards to protect data furnished by the State from unauthorized use or disclosure:

(a.) To limit access to the data only to those employees and officials who need them to perform their official duties in connection with this contract;

(b.) To store the data in an area that is physically safe from access by unauthorized persons;

(c.) To store and process data in such a way that unauthorized persons cannot retrieve the information by means of a computer, remote terminal, or other means;

(d.) To advise all personnel who will have access to the data of the confidential nature of the information, the safeguards required, and the criminal sanctions for noncompliance contained in Federal statutes (such as section 1106(a) of the Social Security Act);

(e.) To ensure, when any authorized Federal or State agency gains access to Social Security records that may have been corrected through the use of State supplied death information, that such agency abides by Federal law and the safeguard provisions contained an agreement with SSA.

The following clause is applicable to non-EDR records and EDR records that did not verify through the contractor's EDRS.

C-6.8 SUMMARY OF VERIFICATION PROCEDURES

(a.) The results of the matching operation are electronically transmitted to the SSA offices servicing the last known address of the beneficiaries identified.

(b.) Each field office first reviews its records to detect recently reported deaths with action pending or recently completed. (The match alert will not be processed in the event that any such action is detected.)

(c.) If no such action is detected, the field office attempts to contact the beneficiary by phone or letter.

(d.) If, as a result of the contact, a family member or other party with reasons to know confirms the match information, termination action is taken by the field office.

(e.) If there is no response to the phone call or mail attempts within a reasonable amount of time, benefits are suspended and the beneficiary is advised in writing that unless he/she contacts SSA, benefits will be terminated by a specified date.

(f.) If someone responds to the contact and purports to be the beneficiary, a certified copy of the death certificate is secured and, if the identifying information indicates that it applies to the beneficiary, a face-to-face meeting is scheduled with the individual who responded to the contact.

(g.) The individual purporting to be the beneficiary is asked to present proof of identity at the meeting. If the field office is satisfied that the SSA beneficiary is alive, no further action is taken. If not, the interview is cancelled and the individual is informed that he/she will be re-contacted. Benefits are then suspended and the case is referred to the Social Security Administration's Office of the Inspector General for inspection. In no case will the match record be the sole basis for terminating any type of benefits. Copies of SSA operating instructions for this process are available upon request.

C-6.9 ISSUANCE OF DELIVERY ORDERS

a. All supplies required under this contract shall be ordered by issuance of delivery orders place against the contract. The Contracting Officer is designated as the only authorized ordering official. Delivery orders will be issued utilizing the following procedure:

   Written delivery orders will be issued by the Contracting Officer on Optional Form (OF) 347, Orders for Supplies or Services. Orders may be issued orally, by fax, or by e-mail.

b. No supplies shall be provided beyond the quantities specified in the written delivery order unless or until and modification or a new delivery order is issued by the Contracting Officer.

Section D - Contract Documents, Exhibits and Attachments

Attachment A – State Death Format

Attachment B -- Table I -- Source Of Death Record State Codes

Attachment C -- Table II-- Place Of Birth Codes State Codes

Attachment D - SSA Death Process Notices

Note: Attachments A, B, C, and D are separate documents.

Section E -- Solicitation Provisions

E-1 FAR Provision 52.212-1, Instructions to Offerors – Commercial Items (June 2008)

In accordance with FAR 12.301 and 12.302, the clause at 52.212-1, is incorporated by reference via Block 27a of the SF 1449.

E-2 Addendum to FAR Provision 52.212-1, Instructions to Offerors – Commercial Items (June 2008)

In accordance with FAR 12.301 and 12.302, the provision at 52.212-1 is hereby tailored by this addendum as follows:

- In paragraph (b)(4) is deleted in its entirety as it has been determined to be not applicable to this solicitation.
- In paragraph (b)(5) is deleted in its entirety as it has been determined to be not applicable to this solicitation.
- In paragraph (b)(10) is deleted in its entirety as it has been determined to be not applicable to this solicitation.
- Paragraph (b)(12) is added to complete and submit Attachment G in Section D.
- In paragraph (d) through (i) and (l) are deleted in their entirety as they have been determined to be not applicable to this solicitation.

E-3 FAR 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS COMMERCIAL ITEMS (MAY 2011)

An offeror shall complete only paragraph (b) of this provision if the offeror has completed the annual representations and certificates electronically at http://orca.bpn.gov. If an offeror has not completed the annual representations and certifications electronically at the ORCA website, the offeror shall complete only paragraphs (c) through (m) of this provision.

(a) *Definitions.* As used in this provision--

"Economically disadvantaged women-owned small business (EDWOSB) concern" means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

"Forced or indentured child labor" means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

"Inverted domestic corporation" means a foreign incorporated entity which is treated as an inverted domestic corporation under 6 U.S.C. 395(b), i.e. a corporation that used to be incorporated in the United States or used to be a partnership in the United States, but now is incorporated in a foreign country, or is a subsidiary whose parent corporation is incorporated in a foreign country, that meets the criteria specified in 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

"Manufactured end product" means any end product in Federal Supply Classes (FSC) 1000-9999, except—

(1) FSC 5510, Lumber and Related Basic Wood Materials;

(2) Federal Supply Group (FSG) 87, Agricultural Supplies;

(3) FSG 88, Live Animals;

(4) FSG 89, Food and Related Consumables;

(5) FSC 9410, Crude Grades of Plant Materials;

(6) FSC 9430, Miscellaneous Crude Animal Products, Inedible;

(7) FSC 9440, Miscellaneous Crude Agricultural and Forestry Products;

(8) FSC 9610, Ores;

(9) FSC 9620, Minerals, Natural and Synthetic; and

(10) FSC 9630, Additive Metal Materials.

"Place of manufacture" means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

"Restricted business operations" means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

"Service-disabled veteran-owned small business concern"—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.

"Veteran-owned small business concern" means a small business concern—

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

"Women-owned business concern" means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

"Women-owned small business concern" means a small business concern --

(1) That is at least 51 percent owned by one or more women or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

"Women-owned small business (WOSB) concern eligible under the WOSB Program" (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally

owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

(b) *Annual Representations and Certifications*

(1) Any changes provided by the offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications posted on the Online Representations and Certifications Application (ORCA) website.

(2) _____ The offeror has completed the annual representations and certifications electronically via the ORCA website at http://orca.bpn.gov. After reviewing the ORCA database information, the offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs _____.

[*Offeror to identify the applicable paragraphs at (c) through (m) of this provision that the offeror has completed for the purposes of this solicitation only, if any.*

These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on ORCA.]

(c) Offerors must complete the following representations when the resulting contract is to be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern*. The offeror represents as part of its offer that it [ ] is, [ ] is not a small business concern.

(2) Veteran-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents as part of its offer that it [ ] is, [ ] is not a veteran-owned small business concern.

(3) Service-disabled veteran-owned small business concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents as part of its offer that it [ ] is, [ ] is not a service-disabled veteran-owned small business concern.

(4) Small disadvantaged business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, for general statistical purposes, that it [ ] is, [ ] is not, a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) Women-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [ ] is, [ ] is not a women-owned small business concern.

Note: Complete paragraphs (c)(6) and (c)(7) only if this solicitation is expected to exceed the simplified acquisition threshold.

(6) WOSB concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The offeror represents that-

(i) It [ ] is, [ ] is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in the circumstances or adverse decision have been issued that affect its eligibility; and

(ii) It [ ] is, [ ] is not a joint venture that complies with the requirement of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of thie provision is accurate in reference to the WOSB Program in (c)(6)(i) of this provision is accurate in reference to the WOSB concern or concerns that are participating in the joint venture. [The offeror shall enter the name or names of the WOSB concern or concerns that are participating in the joint venture: _____.] Each WOSB concern participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.] The offeror represents that-

(i) It [ ] is, [ ] is not an EDWOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and in change in circumstances or adverse decision have been issued that affects its eligibility; and

(ii) It [ ] is, [ ] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(ii) of this provision is accurate in reference to the EDWOSB concern or concerns that are participating in the joint venture. The offeror shall enter the name or names of the EDWOSB concern or concerns that participating the joint venture: _____. Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

(8) Women-owned business concern (other than small business concern). [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.]. The offeror represents that it [ ] is, a women-owned business concern.

(9) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

---

(10) [*Complete only if the solicitation contains the clause at FAR 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns, or FAR 52.2129-25, Small Disadvantaged Business Participation Program – Disadvantaged Status and Reporting, and the offeror desires a benefit based on its disadvantaged status.]*

(i) *General.* The offeror represents that either—

(A) It [ ] is, [ ] is not certified by the Small Business Administration as a small disadvantaged business concern and identified, on the date of this representation, as a certified small disadvantaged business concern in the database maintained by the Small Business Administration (PRO-Net), and that no material change in disadvantaged ownership and control has occurred since its certification, and, where the concern is owned by one or more individuals claiming disadvantaged status, the net worth of each individual upon whom the certification is based does not exceed $750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); or

(B) It [ ] has, [ ] has not submitted a completed application to the Small Business Administration or a Private Certifier to be certified as a small disadvantaged business concern in accordance with 13 CFR 124, Subpart B, and a decision on that application is pending, and that no material change in disadvantaged ownership and control has occurred since its application was submitted.

(ii) *Joint Ventures under the Price Evaluation Adjustment for Small Disadvantaged Business Concerns*. The offeror represents, as part of its offer, that it is a joint venture that complies with the requirements in 13 CFR 124.1002(f) and that the representation in paragraph (c)(9)(i) of this provision is accurate for the small disadvantaged business concern that is participating in the joint venture. [*The offeror shall enter the name of the small disadvantaged business concern that is participating in the joint venture:* _____.]

(11) HUBZone small business concern. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]* The offeror represents, as part of its offer, that--

(i) It [ ] is, [ ] is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material change in ownership and control, principal office, or HUBZone employee percentage has occurred since it was certified by the Small Business Administration in accordance with 13 CFR part 126; and

(ii) It [ ] is, [ ] not a HUBZone joint venture that complies with the requirements of 13 CFR part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for the HUBZone small business concern or concerns that are participating in the joint venture. [*The offeror shall enter the name or names of the HUBZone small business concern or concerns that are participating in the joint venture*: _____.] Each HUBZone small business concern participating in the joint venture shall submit a separate signed copy of the HUBZone representation.

(d) *Representations required to implement provisions of Executive Order 11246* --

(1) Previous contracts and compliance. The offeror represents that --

(i) It [ ] has, [ ] has not, participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It [ ] has, [ ] has not, filed all required compliance reports.

(2) *Affirmative Action Compliance*. The offeror represents that --

(i) It [ ] has developed and has on file, [ ] has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It [ ] has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions (31 U.S.C. 1352).* (Applies only if the contract is expected to exceed $100,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract.

(f) *Buy American Act Certificate.* (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American Act – Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. The terms "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American Act—Supplies."

(2) Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g)(1) *Buy American Act -- Free Trade Agreements -- Israeli Trade Act Certificate.* (Applies only if the clause at FAR 52.225-3, Buy American Act -- Free Trade Agreements -- Israeli Trade Act, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian end product," "component," "domestic end product," "end product," "foreign end product," "Free

Trade Agreement country," and "United States" are defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian or Moroccan end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian or Moroccan End Products) or Israeli End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[*List as necessary*]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) or this provision) as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act."

The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products.

Other Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[*List as necessary*]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American Act—Free Trade Agreements—Israeli Trade Act Certificate, Alternate I.* If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act":

Canadian End Products:

Line Item No.:

_____

[List as necessary]

(3) *Buy American Act—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II.* If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled ``Buy American Act--Free Trade Agreements--Israeli Trade Act'':

Canadian or Israeli End Products:

Line Item No.:	Country of Origin:

[*List as necessary*]

(4) *Trade Agreements Certificate*. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(4)(ii) of this provision, is a U.S.-made or designated country end product as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products

Line Item No.:	Country of Origin:

[*List as necessary*]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American Act. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters (Executive Order 12689)*. (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals--

(1) [ ] Are, [ ] are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency; and

(2) [ ] Have, [ ] have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(3) [ ] Are, [ ] are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses.

(4) [ ] Have, [ ] have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds $3,000 for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) *The tax liability is finally determined*. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) *The taxpayer is delinquent in making payment*. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) *Examples*.

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. §362 (the Bankruptcy Code).

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at* 22.1503 *(b).]*

(1) Listed End Product

Listed End Product	Listed Countries of Origin:

(2) Certification. [*If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]*

[ ] (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

[ ] (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that is has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) [ ] In the United States (Check this box if the total anticipated price of offered end products manufactured outside the united States); or

(2) [ ] Outside the United States.

(k) *Certificates regarding exemptions from the application of the Service Contract Act.* (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [*The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.*]

[ ] (1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1).

The offeror [ ] does [ ] does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

[ ] (2) Certain services as described in FAR 22.1003-4(d)(1).

The offeror [ ] does [ ] does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Act wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l)(1) *Taxpayer Identification Number (TIN) (*26 U.S.C. 6109, *31 U.S.C. 7701)*. (Not applicable if the offeror is required to provide this information to a central contractor registration database to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) *Taxpayer Identification Number (TIN)*.

☐ TIN: _____.

☐ TIN has been applied for.

☐ TIN is not required because:

☐ Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

☐ Offeror is an agency or instrumentality of a foreign government;

☐ Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization*.

☐ Sole proprietorship;

☐ Partnership;

☐ Corporate entity (not tax-exempt);

☐ Corporate entity (tax-exempt);

☐ Government entity (Federal, State, or local);

☐ Foreign government;

☐ International organization per 26 CFR 1.6049-4;

☐ Other _____.

(5) *Common parent*.

☐ Offeror is not owned or controlled by a common parent;

☐ Name and TIN of common parent:

Name _____.

TIN _____.

(m) *Restricted business operations in Sudan*. By submission of its offer, the offeror certifies that it does not conduct any restricted business operations in Sudan.

(n) Prohibition on Contracting with Inverted Domestic Corporations.

(1) A Foreign entity that is treated as an inverted domestic corporation for purposes of the Internal Revenue Code at 26 U.S.C. 7874 (or would be except that the inversion transactions were completed on or before March 4, 2003), is also an inverted domestic corporation for purposes of 6 U.S.C.395 and for this solicitation provision (see FAR 9.108).

(2) Representation. By submission of its offer, the offeror represents that is not an inverted domestic corporation and is not a subsidiary of one.

(o) Sanctioned activities relating to Iran.

(1) Unless a waiver is granted or an exception applies as provided in paragraph (o)(2) of this provision, by submission of its offer, the offeror certifies that the offeror, or any person owned or controlled by the offeror, does not engagae in an activities for which sanctions may be imposed under section 5 of the Iran Sanction Act of 1996.

(2) The certification requirement of paragraph (o)(1) of this provision does not apply if-

(i) This solicitation includes a trade agreements certification (e.g. 52.212-3(g) or a comparable agency provision); and
(ii) the offeror has certified that all offered products to be supplied are designated country end products.

(1) Alternate I (Apr 2011). As prescribed in 12.301(b)(2), add the following paragraph (c)(12) to the basic provision: (*Complete if the offeror has represented itself as disadvantaged in paragraph (c)(4) or (c)(10) of this provision.*)

[*The offeror shall check the category in which its ownership falls*]:

____ Black American.

____ Hispanic American.

____ Native American (American Indians, Eskimos, Aleuts, or Native Hawaiians).

___ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, U.S. Trust Territory of the Pacific Islands (Republic of Palau), Republic of the Marshall Islands, Federated States of Micronesia, the Commonwealth of the Northern Mariana Islands, Guam, Samoa, Macao, Hong Kong, Fiji, Tonga, Kiribati, Tuvalu, or Nauru).

(2) ____ Subcontinent Asian (Asian-Indian) American (persons with origins from India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).

____ Individual/concern, other than one of the preceding.

Alternate II (Apr 2011). As prescribed in 12.301(b)(2), add the following paragraph (c)(10)(iii) to the basic provision:

(iii) *Address*. The offeror represents that its address o is, o is not in a region for which a small disadvantaged business procurement mechanism is authorized and its address has not changed since its certification as a small disadvantaged business concern or submission of its application for certification. The list of authorized small disadvantaged business procurement mechanisms and regions is posted at http://www.arnet.gov/References/sdbadjustments.htm. The offeror shall use the list in effect on the date of this solicitation. "Address," as used in this provision, means the address of the offeror as listed on the Small Business Administration's register of small disadvantaged business concerns or the address on the completed application that the concern has submitted to the Small Business Administration or a Private Certifier in accordance with 13 CFR Part 124, subpart B. For joint ventures, "address" refers to the address of the small disadvantaged business concern that is participating in the joint venture.

E-4 Additional FAR Provisions Incorporated by Full Text

The following FAR provisions are hereby incorporated into this solicitation by full text as follows:

E-4.1 52.209-7 Information Regarding Responsibility Matters (Apr 2010)

(a) Definitions. *As used in this provision—*

"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (*e.g.*, Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than $10,000,000" means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

(b) The offeror [ ] has [ ] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall enter the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the Central Contractor Registration database at http://www.ccr.gov (see 52.204-7).

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

52.216-1 Type of Contract (APR 1984)

The Government contemplates award of an Indefinite-Delivery, Requirements contract resulting from this solicitation. Orders will be issued on a fixed price basis.

E-5 – Additional FAR Provisions Incorporated by Reference

NOT APPLICABLE

E-6 – Additional Agency-Specific Provisions

NOT APPLICABLE

[The statement of Mr. Astrue #2 follows:]

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE 1 OF

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No collect calls)*	8. OFFER DUE DATE/ LOCAL TIME

9. ISSUED BY	CODE	10. THIS ACQUISITION IS ☐ UNRESTRICTED OR ☐ SET ASIDE: % FOR: ☐ SMALL BUSINESS ☐ HUBZONE SMALL BUSINESS ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM ☐ ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) ☐ 8 (A) NAICS: SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE	12. DISCOUNT TERMS	☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING 14. METHOD OF SOLICITATION ☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
TELEPHONE NO.				

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER	18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	(Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN ____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED	☐ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 5/2011)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELPHONE NUMBER OF AUTHORZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NO.	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

STANDARD FORM 1449 (REV. 5/2011) **BACK**

Chairman JOHNSON. Do you think that Social Security could develop a system that could be a source for death information? And should Congress change the law to prevent the Death Master File from being made public?

Mr. ASTRUE. I do believe that Congress should start with the proposition that we should not be releasing this information, except for very specific purposes that the Congress has thought hard about, with protections for the public so that the Federal agencies have full authority to protect the data, as best as possible, if it is used for any other reason. I think the American people really expect no less from us.

Chairman JOHNSON. Thank you, sir. I think that concludes your testimony, and we will proceed to our second panel. And while our witnesses are taking their seats, I just want to thank you for being here, and thank you for the job you are doing over there.

Mr. ASTRUE. Well, thank you. We are really pleased that you have raised this issue, and that you have bipartisan support. And we are looking forward to working with you on the issue.

Chairman JOHNSON. Thank you, sir. The witnesses in the second panel who are taking their seats are Jonathan Agin, from Arlington, Virginia; Stuart Pratt, who is the chief executive officer of the Consumer Data Industry Association; John Breyault, who is the Vice President of Public Policy, Telecommunications and Fraud at the National Consumers League; the Honorable Patrick O'Carroll, who is the Social Security Administration's Inspector General; Dr. Patricia Potrzebowski, Executive Director of the National Association for Public Health Statistics and Information Systems in Silver Spring, Maryland.

You are all seated.

Mr. Agin, welcome. You may proceed.

STATEMENT OF JONATHAN ERIC AGIN, ESQ.
ARLINGTON, VIRGINIA

Mr. AGIN. Good morning, Mr. Chairman, Mr. Becerra, and Members of the Committee. Thank you for inviting me to testify today on this issue that I believe is of vital importance.

Our story begins with the diagnosis of our amazing daughter, Alexis Gina Agin, with a terminal brain tumor on April 10, 2008, when she was just 2 years old. This terrible disease took her life on January 14, 2011, just 2 weeks shy of her fifth birthday. Alexis was and is my hero. Fighting valiantly until the end, she has inspired thousands around the world with her journey.

In 2010, my wife and I traveled with Alexis up and down the East Coast trying several experimental treatments in a desperate attempt to save her life. With each trip, Alexis's medical bills grew. When our 2010 taxes were due, we filed an extension in order to focus on Alexis's treatment, and compiled the vast medical bills that we had.

As we finalized the return in October 2011, I received a call from our accountant to let us know that somebody had stolen Alexis's Social Security number to file a fraudulent tax return. We were forced then to file a paper return, and then prove that Alexis was, in fact, our daughter to proceed with our tax filing.

Thankfully, with the help of our congressional representative, our personal tax situation was resolved favorably.

Within hours of learning of this crime, I personally was contacted by no fewer than 14 other families whose children had died from cancer, and advised that the same thing had happened to them. Since that time, this number has grown significantly. That demonstrates to me that this community is being singularly targeted for this type of theft.

In a matter of 30 seconds, I personally was able to find my daughter's complete Social Security number, birth and date—death dates, full address, and zip code on several websites intended for genealogical research.

After investigating more, we learned about the 1980 and 1982 consent judgment with Mr. Perholtz. It because obvious at that point in time that the Federal Government, through the publication of the Death Master File, was aiding in the commission of this crime. It is my belief that the Federal Government is responsible for providing identity thieves the information to commit this crime.

The common denominator in this story is the Death Master File. The Social Security Administration, as you have just heard from the Commissioner, makes this Death Master File publicly available to anybody who wishes to purchase it. Some of the intended recipients are government agencies. And some are services which allow people to do genealogical research. Some of these purchasers make the information free and available to anybody with a computer.

As a taxpayer and a parent of a child who passed away from cancer, I am outraged that the most private information of our children is being made commercially available. Not only is this an invasion of my child's privacy, but it adds to the tremendous grief that my wife and I live with on a daily basis. While trivial to some, Alexis's Social Security number is one of the only things that we have left of her identity.

Recently, the IRS estimated that approximately 350,000 fraudulent filings occurred in 2010. According to IRS officials, these fraudulent filings claimed $1.25 billion in refunds.

One of the problems is that the Federal Government, as we have heard, is disclosing more information than is necessary, pursuant to the terms of the consent judgement. In June 2008, as we have heard, the Inspector General of the Social Security Administration issued a very critical report detailing how publication of the Death Master File, or the DMF, has resulted in the breach of citizens' personally-identifiable information. The report concludes that the Social Security Administration discloses far more detailed personal information in the DMF than required under the original consent judgement.

H.R. 3475 is a solution to a significant problem that affects not only grieving parents, but every family who loses a loved one. Some argue that this bill will not stop widespread fraud. Some argue that the DMF is critical to combat and conduct genealogical research. This bill is not intended to prevent or limit the lawful use of the DMF, and I think that is an important distinction that everybody needs to understand. Nobody is trying to limit the availability of the DMF to track down fraud. My point is that we need

to limit it to ensure that nobody else has to suffer as my wife and the vast number of cancer families have suffered.

In closing, this is not a victimless crime. My daughter is a victim. She was victimized twice, once by the cancer that stole her from this Earth, and then by a coldhearted criminal who stalked her and utilized her death for profit. It disgusts me to no end to know that somebody preyed upon my daughter's death for his or her own gain. It is nothing short of a despicable crime. And the release of Alexis's complete Social Security number and other personal identifiers in the DMF to the general public facilitated this crime. I have no doubt of that.

This simply is not an emotionally-charged issue, as some argue. Fraud is not something that we simply should accept as a necessary consequence of easy access to information. It is time that this loophole is closed, and this legislation is the manner in which to accomplish this aim. It is simple and to the point. And in this era, when our government is struggling to find ways to save money for the taxpayer, it is a very easy fix with little to no consequences, repercussions, or detriment to the citizens of this country.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Agin follows:]

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

CONGRESSIONAL TESTIMONY

FROM: **Jonathan Eric Agin, Esq.**
TO: **House Ways and Means Committee, Subcommittee on Social Security**
DATE: **February 2, 2012**
RE: **H.R. 3475**

Good morning Mr. Chairman and members of the Committee. Thank you for allowing me to be here today to testify on this issue of vital importance.

My family's story begins with the diagnosis of our amazing daughter, Alexis Gina Agin, with a terminal brain tumor at the age of two on April 10, 2008. Ultimately, this terrible disease took her life on January 14, 2011, just two weeks shy of her fifth birthday. Alexis was and is my hero. Fighting valiantly until the end, she has inspired thousands around the world with her journey.

In 2010, my wife and I travelled with Alexis up and down the East Coast trying several experimental treatments, in a desperate attempt to save her. With each trip, Alexis' medical bills mounted. When it came time to file our 2010 taxes, compiling all of our receipts for the medical expenses was time-consuming and emotionally draining. Accordingly, my wife and I, through our accountant, filed with the IRS for an extension. In October 2011, after completing the difficult and grueling task of finalizing our 2010 taxes, I received a telephone call from our accountant advising us that someone had already filed a tax return for 2010 using Alexis' social security number. Beyond being completely stunned at that very moment, we were advised that we would not be able to file an electronic return. Instead, our accountant would have to complete the paper forms and file them in the traditional manner. More importantly for purposes of HR 3475, he told us that we ultimately would have to prove that our deceased daughter was, in fact, our daughter. In situations involving this type of criminal fraud, the IRS credits the first filer and presumes that the initial filing is accurate.

That same day, we reached out to the community of grieving cancer parents that we have come to know since April 2008 and told them what had happened. With incredulous amazement, we learned within a single hour of no fewer than fourteen other families whose children had died and also had experienced the additional travesty of their child's social security number being stolen. Clearly we were not alone. We then learned through our own research and from other parents that this is, in fact, a very widespread issue impacting parents who lose a child due to any and all reasons imaginable.

Not surprisingly, when I first learned that Alexis' social security number had been fraudulently used, I wanted to know how someone could have found it. Within a matter of seconds on the internet, I was able to locate her complete social security number and other personal identifying information, including her birth and death dates, on several websites intended for genealogical research. I immediately contacted one of the services, who directed

me to the service's outside counsel. When I asked the attorney to remove my daughter's personal information from the website, he advised me that the service was within its legal rights to display the information and that it refused to remove her social security number. The attorney cited as support for their position a 1980 consent judgment between the United States Government and a private citizen, Ronald Perholtz. It was at that point that we truly realized how significant this problem is, and more importantly, how the federal government is partly to blame. It is my belief that the federal government is responsible for providing identity thieves the information required to commit this costly crime. By affording widespread access to this type of information, the federal government provides the perfect platform for the commission of this crime.

The common denominator in this story is the Death Master File (hereinafter "DMF"). The Social Security Administration makes the DMF available to the National Technical Information Service (NTIS) of the Department of Commerce, who then sells the DMF to private and public sector customers, including government agencies, financial institutions, investigative entities, credit reporting organizations, genealogical researchers and other industries. Some of these purchasers, namely organizations hosting websites aimed at facilitating genealogical research, then make available the DMF for free to the public at large. It therefore is available to nearly anyone and perpetuates identity theft and fraud against the federal and state governments at astronomical levels. As a taxpayer and parent of a child who passed away from cancer, I am outraged at the most private information of our children being made commercially available. Not only is this a significant invasion of my child's privacy, but it adds to the tremendous grief that my wife and I live with on a daily basis and will continue to live with for the rest of our lives. While it may seem trivial to some, Alexis' social security number is one of the only things that we have left of her identity. Thus, the theft of it robbed us of something truly priceless.

Due to an ongoing media probe and public pressure, the IRS for the first time recently responded to inquiries on this issue, and estimated that there were approximately 350,000 fraudulent tax filings in 2010. According to IRS officials, these fraudulent filings claimed $1.25 billion in refunds.[1] The cost to the federal government to investigate and prosecute that magnitude of fraud could be spent in much better ways, including research to fund cures for our children.

In addition, it is worth noting that the federal government discloses far more information than is required under the 1980 settlement. In June 2008, the Inspector General of the Social Security Administration issued a critical report detailing how publication of the DMF has resulted in the breach of citizens' personally identifiable information.[2] The report concludes that the Social Security Administration "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

---

[1] Dale McFeatters, Govt. shares blame as ID theft worsens, available at *http://bostonherald.com/news/opinion/op_ed/view/2011_1105govt_shares_blame_as_id_theft_worsens* (November 5, 2011).

[2] Office of the Inspector General, Social Security Administration, *Personally Identifiable Information Made Available to the General Public Via the Death master File*, Audit Report A-06-08-18042 (June 2008).

published in the DMF to include the decedent's date of birth, first and middle name, and last known residential state/zip code."[3] The report's conclusion is simple: less information should be released, and greater efforts at accuracy and protection must be taken.

Significantly, Ronald Perholtz, the man who filed the lawsuit that led to the 1980 consent judgment resulting in creation of the DMF, sought release of the information to help reduce fraud. Specifically, he wanted the information as a tool for pension companies to identify theft of pension benefits. Soon after learning the DMF was created, Mr. Perholtz learned that the DMF frequently listed the social security numbers of people who were not, in fact, dead.[4] Now, he believes that changes need to be made in order to stop this type of fraud. Indeed, Mr. Perholtz stated that he is willing to renegotiate the original settlement as he feels so strongly that the DMF is being abused.[5]

H.R. 3475 is a solution to a significant problem that affects not only grieving parents, but also every family who loses a loved one. It also is a solution to a problem that was never anticipated, and would eliminate dissemination by the federal government of extraneous information that it is not required to release. This additional information, along with the readily accessible nature of individuals' social security numbers, has provided identity thieves an avenue to commit this crime and defraud the taxpayers and government.

Those who argue that the release of this information is critical to combat fraud and conduct genealogical research fail to understand that this Bill is not intended to prevent or limit the lawful use of Social Security Numbers or genealogical research. First, I would say to any individual conducting genealogical research, why do you need to know my daughter's social security number? Why should it be publicly available to anyone with a computer? What purpose does her full social security number, along with her birth and death dates, address, and other personal identifying information have for your familial research? The clear answer is that it has absolutely no purpose. Alexis didn't die a long time ago—she died last year. While it may be difficult to find information about your ancestors from generations ago, it should not be hard to confirm your familial connection (or lack thereof) to someone born just six years ago.

More importantly, this Bill will not prevent credit bureaus and financial institutions from fulfilling their charge of protecting us from fraud. To the contrary, because access to this information will be more restricted, these institutions will be more empowered knowing that the potential incidence rates of identity theft and fraud will be curtailed. Potentially far fewer instances of fraud against lawful citizens will be committed, thus reducing the amount of investigation necessary. The intent of this legislation is not to limit or prohibit financial institutions from investigating fraud; rather it is to prohibit the widespread publication and easy access of personal information that is utilized by criminals to defraud the government. As for hospitals and other institutions who claim to utilize the DMF to determine if their patients are deceased, I submit that there are other far less destructive methods to make such determinations and conduct your research. Again, this Bill is not aimed at those who have a legitimate need for

---

[3] *Id*. at 6.
[4] Thomas Hargrove, Social Security 'Death File' designed to fight fraud but now aids it, available at *www.scrippsnews.com* (November 14, 2011).
[5] *Id*.

access to individuals' social security numbers and they will continue to have access to this information.

I have been told that in most cases, the government does not have the resources to prosecute this crime. It either is too costly, or the government simply does not have the ability to track and punish those who are stealing from it and taxpayers alike. If this crime was prevented, to the best extent possible upfront with this simple measure, there would be little concern regarding the cost to prosecute as more resources could be made available, stiffer penalties proscribed and additional deterrents fully understood.

In closing, this is not a victimless crime. My daughter is a victim. She was victimized twice. Once by the cancer that stole her from this earth, and then by a cold-hearted criminal who stalked her and utilized her death for profit. It disgusts me to no end to know that someone prayed upon my daughter's death for his or her own gain. It is an added insult for a grieving parent. It is nothing short of a despicable crime and the release of Alexis' complete social security number and other personal identifiers to the general public facilitated this crime. But this simply is not an emotionally charged issue, as some argue. Fraud is not something that we simply should accept as a necessary consequence of easy access to information. Yes, security breaches will always be possible regardless of the measures that we put into place. But when there is a simple fix to a significant problem that affects all taxpayers, the fix should be taken seriously and enacted with haste. It is time that this loophole is closed and this legislation is the manner in which to accomplish this aim. Nothing short of this will accomplish the task. It is simple and to the point, and in this era when our government is struggling to find ways to save money for the taxpayer, it is a very easy fix with little to no consequences or repercussions to citizens of this country.

Thank you Mr. Chairman and distinguished members of the Committee.

Jonathan Eric Agin

Chairman JOHNSON. Thank you, sir. That is a beautiful girl.
Mr. AGIN. Thank you.
Chairman JOHNSON. Mr. Pratt, welcome. Please go ahead.

STATEMENT OF STUART K. PRATT, CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION

Mr. PRATT. Mr. Chairman, Ranking Member Becerra, Members of the Committee, thank you for the chance to appear and testify. Thank you for holding this hearing. And, candidly, thank you for the opportunity for the CDIA and its members to contribute to solving the problem, so that we don't have other families who have suffered the way the Agins have suffered. And that is, I think, the balance that we are looking for.

Mr. Becerra, in many ways, some of the questions you asked in the first round of testimony are just right on. And really, without going through all the testimony that we have submitted for the record, there are important uses for the Death Master File.

In our world, it is a business-to-business transaction. In our world, it is a contractual transaction. In our world, it is a secured and closed transaction. And in our world, it is a nonpublic use. So the information and the data itself is subject to information security standards. So, in our world, it is using the Death Master File to stop identity theft, to stop entitlement fraud, to stop—to enable a life insurance company—in fact, in some cases, by law, but in most States not—to track down individuals who are the beneficiaries of life insurance, to ensure that claims are processed properly and effectively and quickly for individuals who have lost a loved one.

Our members deliver approximately—our members' data is involved in probably 9 billion transactions every year in the United States. We are probably the best channel of distribution for this kind of information in a private sector marketplace, to make sure that the data is used quickly. In fact, I testified on this very topic right after 9/11. The Commissioner mentioned this issue in his testimony, as well.

And, in fact, we were involved in working with the Department of Commerce, and our own members were involved in working to ramp up the speed with which we could, in a secure manner, get the Death Master File, move it into data centers so that it could be used for all of these types of transactions we have just discussed.

In our view, it is not the use of the Death Master File in the business-to-business context which is creating the risk. That is the reason we are here, and that is the reason we have already had some meetings with staff to explain how we think the bill could be clarified, to make sure that appropriate uses are codified, and that you can still protect the Death Master File from otherwise being subject to a Freedom of Information Act type of request that makes it available to anyone. We would support amendments to do that.

We appreciate this opportunity to testify, and I am honored to be on the panel with Mr. Agin. Thank you.

[The prepared statement of Mr. Pratt follows:]

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

STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

HEARING ON

THE ACCURACY AND USES OF THE DEATH MASTER FILE

Before the Subcommittee on Social Security of the House Ways and Means Committee

of the

United States House of Representatives

Washington, D.C.

Thursday, February 2, 2012

Chairman Johnson, thank you for this opportunity to appear before the House Ways and Means Subcommittee on Social Security. For the record, my name is Stuart Pratt and I am President of the Consumer Data Industry Association.

CDIA is an international trade association with more than 190 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' products and services ensure that consumers can engage in fair and safe transactions, enjoy broader competition leading to better prices and to access a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

Today, my testimony will focus on two important points:

- The beneficial uses of the Social Security Administration's Death Master File (DMF) which need to be preserved, and the consequences of cutting off access.
- Changes to the DMF that reduce its completeness.

Before I address these two points it is important to know that our members' products are subject to a number of federal laws that regulate the use of consumer data. For example many CDIA members are financial institutions regulated by Title V of the Gramm-Leach-Bliley Act. All members operate a consumer reporting agency regulated by the Fair Credit Reporting Act. Other laws may apply, as well.

Beneficial Uses of the DMF by CDIA Members:

Now let me turn to the beneficial uses of the DMF and let's start with fraud prevention.

Banks, employers, insurance companies, the healthcare industry and the government all rely on data obtained from the DMF to identify deceased individuals in order to identify and ultimately prevent fraud. Our members are the technological bridge between DMF data and billions of consumer transactions. It is our private sector members that have ensured that the DMF data is available where it is needed in the US economy.

As an example our members which operate nationwide consumer reporting agencies obtain DMF data and load it into the databases used to produce credit reports. These data bases contain more than 200 million files on credit-active Americans. By loading the DMF it is delivered along with credit reports so that creditors are made aware that a potential application is associated with a person whose social is on the DMF or that a current customer is deceased. One of our members shared with us that in a recent review of financial transactions in a financial services portfolio 45 percent of transactions

connected to records of deceased persons were found to be fraudulent. Preventing this type of identity theft relieves surviving relatives of the burden of dealing with fraudulent accounts resulting from misuse of their lost loved ones and saves financial institutions tens of millions of dollars each year.

Insurance companies similarly detect and prevent claims fraud by identifying benefits claims from and payments to deceased individuals. Fraud schemes have been identified using the names of deceased healthcare providers, including having claims submitted in their name. Within a disability insurance carrier's portfolio, fraudulent claims paid to deceased individuals can be as high as .1%; this represents a significant amount of money being fraudulently collected.

The benefits for healthcare providers are no different than for the financial services or insurance industries. Knowing that someone is attempting to access healthcare using the identity of a deceased individual can prevent losses and confusion for relatives of the deceased.

Government agencies providing benefits and entitlements are under attack by fraudsters that make use of the identities of deceased individuals. Benefit payments, tax refunds, and other programs are exposed; by using DMF data and data analytics it is possible to uncover many of these schemes.

Beyond fraud there are other beneficial uses. Life insurance companies need access to reliable, comprehensive records identifying individuals known to have died. In the past life insurance companies have waited until being contacted by a policy owner, beneficiary, or estate before beginning the process of verifying a death, locating beneficiaries, and paying proceeds.

Today, life insurance companies are under increasing pressure in the states to proactively monitor the status of insureds and to proactively begin the process of verifying death, identifying and locating beneficiaries, and paying out insurance proceeds. Life insurance companies are required by several states to match their in-force and lapsed policies against the SSA DMF to determine whether there are deceased insureds for which policy proceeds have not been paid. If access to the DMF is eliminated, then these carriers could not comply with the state mandates to conduct the required searches.

Lenders and the receivables management industry (first party and third party collections) use data from the DMF in order to appropriately handle indebted, deceased customers. For example, accounts in collections which are associated with deceased individuals are handled differently from other accounts. This special handling includes both the sentimental and legal manner in which the bank or agency approaches collection, and a decision as to whether to attempt collection at all.

Allowing CDIA's members to access the DMF in order for them to distribute it across the US economy brings clear benefits. Cutting off our members' access to the DMF will empower criminals.

Thieves are not perpetrating these crimes using DMF data. According to the Privacy Rights Clearing House identity thieves obtain information about deceased individuals in various ways including:

- Watching the obituaries and engaging in pretexting to obtain critical identifying information.
- Stealing or ordering death certificates
- The thief may also be a family member who may take advantage of the situation or who has already been using that identity. This may be especially true if the deceased suffered from lengthy illness, mental confusion, or if there is disagreement among family members prior to the death.

There are few options for preventing fraud and ensuring legal compliance if the DMF is cut off. In fact, while the DMF is made available today as a result of a 1978 Freedom of Information Act (FOIA) lawsuit filed in Federal District Court, it is the position of the CDIA that appropriate access to the DMF should be codified into law and not left to future interpretations of FOIA.

The Completeness of DMF

In 2002 the Social Security Administration began disclosing certain state records on the public DMF. However the SSA subsequently determined that it can no longer disclose protected state records. The SSA points out that Section 205(r) of the Social Security Act prohibits the SSA from disclosing State death records received through contracts with the states (some limited exceptions apply).

In terms of the effect on the DMF the SSA reports that the historical Public DMF contains 89 million records. SSA will remove approximately 4.2 million records from this file and add about 1 million fewer records annually. This loss of 1 million records is consequential since our members estimate that this is approximately 35% of all new records added each year.

We believe that in addition to codifying into law the appropriate access to the DMF, we also believe that Section 205(r) of the Social Security Act should be amended to allow for this access to include all state death records as part of disclosure.

Conclusion

In closing let me emphasize some important points:

- Uses of the DMF for fraud prevention, legal compliance processes and for ensuring US businesses are aware of the status of their customers is not facilitating identity theft.

- There is no substitute for the DMF available in the marketplace. If the DMF is not available US businesses will experience an increase in fraud and in some cases fail to comply with other state or federal requirements.
- Identity thieves are not obtaining access to the DMF via our members' business-to-business distribution of it. Our members vet their customers carefully and the distribution of the DMF often is in conjunction with products regulated by other federal laws such as the FCRA or GLB Title V.

We urge the Committee to consider amending the Social Security Act to codify appropriate business-to-business access and distribution of the DMF, including state records that cannot be disclosed today due to the SSA's interpretation of Section 205(r) of the Social Security Act.

Thank you again for this opportunity to appear before your committee. We look forward to working with your committee going forward and I am happy to answer any questions.

Chairman JOHNSON. Thank you, sir. I appreciate your testimony.

Mr. Breyault, welcome. You may proceed, sir.

STATEMENT OF JOHN D. BREYAULT, VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS AND FRAUD, NATIONAL CONSUMERS LEAGUE

Mr. BREYAULT. Good morning, Mr. Chairman, Ranking Member Becerra, and Members of the Subcommittee. My name is John Breyault, and I am Vice President of Public Policy, Telecommunications and Fraud for the National Consumers League.

Founded in 1899, NCL is the Nation's oldest consumer organization. Our nonprofit mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. I greatly appreciate the opportunity to discuss the impact that the misuse of the Social Security Administration's Death Master File data has on consumers.

As the director of NCL's fraud center, I hear on a daily basis about the personal and financial toll that identity theft and other fraud takes on consumers and their families. The statistics are sobering. In 2011 we received nearly 9,000 complaints from victims of a variety of scams. Consumers reporting fraud to NCL lost, on average, $990. And, in many cases, these unscrupulous con artists financially ruined their victims.

NCL statistics represent only a small fraction of the fraud problem, however. In 2010, the Federal Trade Commission received over 1.3 million complaints, of which more than 250,000 involved identity theft. And even that number represents only those victims who knew enough to complain to the FTC. According to one estimate, 8.1 million adults were victims of identity theft in 2010, with each incident costing $631 to resolve.

Despite these numbers, it never ceases to amaze me, the lengths to which scam artists will go to defraud consumers. As the father of two young daughters, the reports I have seen of the misuse of dead children's identities to commit tax fraud sickens me. The vulnerability of children to identity theft is well established. It is estimated that as many as 140,000 minors fall victim to ID fraud annually. According to Carnegie Mellon researchers, 10.2 percent of children have had their Social Security number misused by someone else, a rate 51 times higher than the rate for adults.

While it is unknown how many deceased children's identities have been used to commit tax fraud, the volume of news reports about this scam, and anecdotal evidence from their parents, such as Mr. Agin, suggest it is not limited to a few isolated cases. It is also clear that by using websites that publish DMF data, identity thieves can quickly and cheaply gain access to recently-deceased children's full names, dates of birth, and full Social Security numbers: the so-called holy trinity of personally-identifying information.

Clearly, the role that the public availability of the SSA's DMF data plays in these scams requires additional study. Consumers are also harmed when they are mistakenly listed as deceased on the DMF. The SSA has stated that approximately 14,000 living Americans are affected by these errors annually. Such mistakes can lead to frozen bank accounts, canceled cell phone service, loan denials,

and refused job interviews. It can require months for the SSA to correct these errors. And even then, living individuals' personally-identifiable information may still be exposed.

The public availability of the SSA's DMF data is certainly not the sole driver of identity theft. Indeed, many organizations use DMF data regularly to deter fraud, administer pension benefits, and conduct medical research, among other uses. That said, it is clear that reform is needed to address the likelihood that identity thieves will continue to make use of the public DMF to harm consumers.

While NCL generally supports transparency of government data, in this case we believe that the risk that the public DMF could be used for nefarious purposes outweighs the benefit. However, in the interest of protecting legitimate uses of the DMF, we do not believe that a total ban on the sale of this data would be in the best interest of consumers. Instead, we would urge Congress and the SSA to undertake a number of reforms.

First, personally-identifiable information included in the public DMF should be limited, and alternatives to the inclusion of the full Social Security number in the file should be explored.

Second, living Americans who have been mistakenly listed in the DMF should be notified that their personally-identifiable information may have been compromised, and steps to safeguard their identities should be recommended.

Third, access to the DMF should be restricted to organizations that can certify they have a legitimate need for the information, such as for fraud prevention, or benefits administration purposes.

Fourth, penalties should be increased for DMF recipients who fail to keep DMF data up to date, or who misuse or redisclose DMF information.

Finally, the SSA should undertake a study, in conjunction with DMF data recipients, to evaluate the usefulness of DMF data in preventing identity theft.

In conclusion, I would like to take this opportunity once again to thank you, Mr. Chairman and the Members of the Subcommittee, for inviting me to testify today on behalf of the National Consumers League, and consumers nationwide.

I look forward to answering your questions.

Thank you.

[The prepared statement of Mr. Breyault follows:]

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

TESTIMONY BEFORE THE HOUSE OF WAYS AND MEANS COMMITTEE'S

SUBCOMMITTEE ON SOCIAL SECURITY

"HEARING ON SOCIAL SECURITY'S DEATH RECORDS"

FEBRUARY 2, 2012

9:00 A.M.

JOHN D. BREYAULT

VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS AND FRAUD

NATIONAL CONSUMERS LEAGUE

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

Good morning Mr. Chairman, Ranking Member Becerra and members of the subcommittee. My name is John Breyault and I am the Vice President of Public Policy, Telecommunications and Fraud for the National Consumers League (NCL).

Founded in 1899, NCL is the nation's oldest consumer organization. Our non-profit mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. NCL's connection to the Social Security Administration runs deep. Frances Perkins, who was elected Secretary of the League in 1910, was the nation's first female Cabinet member and was one of the architects of the Social Security Act of 1935.

I greatly appreciate the opportunity to discuss the issue of Social Security's death records and the impact the misuse of these records has on consumers. As the Director of NCL's Fraud Center, I hear on a daily basis about the personal and financial toll that identity theft and other fraud takes on consumers and their families. In 2011, we received nearly 9,000 complaints from victims of a variety of fraud. Consumers reporting fraud to NCL lost, on average, $990.[1] In many cases, these unscrupulous con artists financially ruined their victims. NCL's statistics represent only a small fraction of the fraud problem. For example, in 2012, the Federal Trade Commission received over 1.3 million complaints, of which more than 250,000 involved identity theft.[2] And that represents only those who knew enough to complain to the FTC. According to research firm Javelin Strategy, 8.1 million adults were victims of identity theft in 2010, with each incident costing $631 to resolve.[3]

---

[1] Source: NCL fraud complaint statistics, 2011.
[2] Federal Trade Commission. *Consumer Sentinel Network Data Book for January-December 2010*. Pgs. 3, 5. March 2011. Available online: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf
[3] Saranow Schultz, Jennifer. "The Rising Cost of Identity Theft for Consumers," *New York Times*. February 9, 2011. Online: http://bucks.blogs.nytimes.com/2011/02/09/the-rising-cost-of-identity-theft-for-consumers/

Despite these sobering statistics, it never ceases to amaze me the extent to which scam artists will go to defraud consumers. As a father of two young daughters, the reports I have seen of the misuse of dead children's personal information to commit identity theft sickens me.

The vulnerability of children to identity theft is well established. According to recent estimates, 140,000 identity frauds are perpetrated on minors each year.[4] According to researchers at Carnegie Mellon University, 10.2% of children have had their Social Security Number used by someone else – 51 times higher than the 0.2% rate for adults.[5] While it is unknown how many deceased children's identities scam artists have misappropriated, the volume of news articles about this scam and anecdotal evidence from parents of the deceased children suggest it is not limited to a few isolated cases.[6]

The role that the public availability of the Social Security Administration's Death Master File (DMF) plays in these scams requires additional study. However, it is clear that identity thieves can quickly and cheaply gain access online to the so-called "holy trinity" of identifying information of recently deceased children – full name, date of birth and full Social Security Number – using websites that access DMF data. On its face, the public availability of a remarkably complete set of personally identifiable information of 83 million deceased Americans for as little as $995 is extremely troubling.

Additional consumer harm arises when individuals are mistakenly listed as deceased on the DMF. Due to "inadvertent keying errors" by federal workers

---

[4] I.D. Analytics. "More Than 140,000 Children Could Be Victims of Identity Fraud Each Year," Press release. July 12, 2011. Online: http://www.idanalytics.com/news-and-events/news-releases/2011/7-12-2011.php

[5] Power, Richard. "Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers," Carnegie Mellon Cylab at 4. April 1, 2011. Online: http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf

[6] See e.g. Goldberg, Eleanor. "Why Thieves Are Stealing Childhood Cancer Victims' Identities," Huffington Post. November 18, 2011. Online: http://www.huffingtonpost.com/2011/11/17/why-thieves-are-stealing-childhood-cancer-victims-identities_n_1093481.html

entering death information, the Social Security Administration has stated that approximately 14,000 living Americans are listed as deceased in the DMF annually.[7] Such mistakes can lead to frozen bank accounts, cancelled cell phone service, loan denials and refused job interviews.[8] Due to the DMF's public availability, these individuals are also put at increased risk of identity theft. It may require months for the SSA to correct these errors and even then, living individuals' personally identifiable information may still be exposed.[9]

The public availability of the Social Security Administration's DMF data is certainly not the sole driver of identity theft. Indeed, its wide availability has clearly benefitted security firms that use it to deter fraud.[10] In addition, pension funds, insurance organizations, and medical researchers use DMF data for completely legitimate reasons.[11] That said, it is clear that reform is needed to address the likelihood that identity thieves will continue to make use of the DMF to harm consumers. We also believe that more should also be done to alert consumers who are falsely listed as deceased on the DMF so that they can take action to protect their identities.

A number of commentators, including the SSA's Office of Inspector General[12] and the Internal Revenue Service's National Taxpayer Advocate[13] have recommended ways

---

[7] Hargrove, Thomas. "Grave mistakes: SSA silent on private data breach," Scripps Howard News Service. November 6, 2011. Online: http://www.courierpress.com/news/2011/nov/06/grave-mistakes-ssa-silent-on-private-data-breach/?print=1

[8] Id.

[9] Social Security Administration. "Personally Identifiable Information Made Available to the General Public Via the Death Master File," Office of the Inspector General Audit Report. Pgs. 4-5. June 2008. Online: http://oig.ssa.gov/sites/default/files/audit/full/pdf/A-06-08-18042.pdf

[10] See e.g. ID Analytics. "Keep the Death Master File alive," Blog posting. December 21, 2011. Online: http://idanalytics.com/idalabs/2011/keep-the-death-master-file-alive/ (stating that "We use this SSA Death Master File as an upfront defense to weed out such applications, and our process successfully stops these attempts.").

[11] National Technical Information Service. "Social Security Administration's Death Master File." Online: http://www.ntis.gov/products/ssa-dmf.aspx

[12] See generally, Social Security Administration. "Personally Identifiable Information Made Available to the General Public Via the Death Master File," Office of the Inspector General Audit Report. June 2008. Online: http://oig.ssa.gov/sites/default/files/audit/full/pdf/A-06-08-18042.pdf

to better protect consumers from identity theft stemming from personally identifiable information made available via the DMF. Several reforms that the National Consumers League supports include:

- Limiting the personally identifiable information included in the public DMF to the absolute minimum required and exploring alternatives to the inclusion of the full Social Security Number;

- Notifying living consumers who have been mistakenly listed in the DMF that their personally identifiable information may have been compromised and recommending steps to safeguard their identities;

- Restricting access to certain personally identifiable information in the DMF to organizations that can certify that have a legitimate need for the information for fraud prevention or benefits administration purposes;

- Increasing penalties for failure of DMF recipients to keep DMF data up to date or the misuse or re-disclosure of DMF information; and

- Requiring the SSA to undertake a study, in conjunction with DMF data recipients, of the usefulness of DMF data in preventing identity theft.

While NCL generally supports transparency of government data, in this case, we believe that the risk that publicly available DMF data could be used for nefarious purposes outweighs the benefit. However, in the interest of the timely provision of survivor benefits and the use of this data for fraud protection efforts, we would not support a total ban on the sale of DMF data. Instead, we believe that SSA and the Department of Commerce should take steps to ensure that DMF data is made

[13] See Legislative Recommendation: Restrict Access to the Death Master File, infra. See also Identify Theft and Tax Fraud Prevention Act, S. 1534, 112th Cong. § 9 (1st Sess. 2011) Online: http://www.taxpayeradvocate.irs.gov/userfiles/file/2011_ARC_MSP%203.pdf

available only to organizations that can demonstrate a legitimate need. DMF data recipients should likewise be held to a higher standard of accountability for maintaining the integrity and security of this sensitive data.

In conclusion, I would like to take this opportunity to once again thank the members of the subcommittee for inviting me to testify today on behalf of the National Consumers League and consumers nationwide.

Chairman JOHNSON. Thank you, sir. I appreciate your testimony.

Mr. O'Carroll, you are recognized. Thank you for being here.

STATEMENT OF HON. PATRICK P. O'CARROLL, JR.
INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. O'CARROLL. Good morning, Chairman Johnson, Mr. Becerra, Mr. Marchant, and Members of the Subcommittee. Thank you for this invitation to testify today.

My office believes that limiting public access to the agency's Death Master File, or DMF, to what is required by law, and taking all possible steps to ensure the file's accuracy are critical elements in preventing SSN misuse and identity theft.

Only Congress is authorized to alter what the law requires, so my office works closely with SSA on the second element, ensuring the accuracy of the DMF.

We have conducted multiple audits and made many recommendations with this obligation in mind. In a 2008 report on SSA's death records, we reported that thousands of living individuals were mistakenly listed as deceased on the DMF. These errors can have a serious financial impact on the affected individuals, and the errors can lead to identity theft.

To protect personal information and improve SSN integrity, we recommended that SSA consider implementing a several-month delay in the release of the DMF updates, so the agency could correct erroneous death entries before they are made public; limit the amount of information included on the DMF to the absolute minimum required by law; and explore alternatives to the inclusion of a person's full SSN on the DMF.

The agency has not taken action on these recommendations for the following reasons: SSA said government and financial organizations depend on the DMF data to combat fraud and identity theft, so they must have timely, up-to-date death information; and SSA said that the DMF data does not have to be limited to what the law requires, because a deceased individual does not have privacy rights, according to the Freedom of Information Act.

There are about 1,000 cases each month in which a living individual is mistakenly included in the DMF. We have found that these errors usually occurred when SSA processed death information that came from a family member or a funeral home. SSA said it moves quickly to correct the situation when errors occur. The agency reports it has not found evidence of past data misuse. However, we remain concerned that these errors can lead to premature benefit termination and cause financial hardship and distress.

Death Master Files with active SSNs belonging to living persons can serve as a source of information that would be useful in committing SSN misuse and identity theft. DMF updates reveal to potential criminals the personal information of individuals who are alive. The information could be used to apply for credit or benefits, or assume a whole new identity.

Limiting or discontinuing the availability of the DMF is a serious legislative and policy decision for Congress and the SSA. In November 2011, Chairman Johnson and several Members of the Subcommittee introduced the Keeping IDs Safe Act. The bill would end

the sale of the DMF to the public. The public distribution of SSA's death records raises serious concerns.

Valid SSNs can, in essence, be purchased from the government by clever identity thieves. However, DMF data has important productive uses in government and in the financial industry, including verifying deaths, ensuring benefit payment accuracy, and identifying and preventing ID theft. The SSN's key uses in government and finance make the SSN a valuable commodity for criminals. And both SSN misuse and identity theft remain a significant public risk. Failure to take action creates an unnecessary public hazard.

In conclusion, we encourage efforts to limit public access to the DMF through legislative or policy changes, such as the Keeping the IDs Safe Act. Pending such changes, we will continue to examine the issue and recommend steps to limit the information made available to the extent permitted by law, and advocate a risk-based approach to the distribution of the DMF.

We look forward to continuing to work with the Subcommittee and SSA in these and future efforts to protect personal information, and to prevent identity theft. Thank you for this invitation to testify today, and I will be happy to answer any questions.

[The prepared statement of Mr. O'Carroll follows:]

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 genealogy.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.

Chairman JOHNSON. Thank you, sir. I appreciate your testimony. I hope we can resolve that. I didn't realize until we got started on this that Social Security was responsible for that Death File. You know, it seems to me if Commerce is selling it, they ought to be responsible for it, or the States, not Social Security. Do you agree?

Mr. O'CARROLL. Or just restricting the use, in general——

Chairman JOHNSON. Yes.

Mr. O'CARROLL [continuing]. Is what——

Chairman JOHNSON. Thank you.

Mr. O'CARROLL [continuing]. Helpful.

Chairman JOHNSON. Dr. Potrzebowski?

Ms. POTRZEBOWSKI. Very good.

Chairman JOHNSON. Got it.

[Laughter.]

Ms. POTRZEBOWSKI. Thank you.

Chairman JOHNSON. You are recognized. Please go ahead. Thank you.

STATEMENT OF PATRICIA W. POTRZEBOWSKI, PH.D., EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION FOR PUBLIC HEALTH STATISTICS AND INFORMATION SYSTEMS, SILVER SPRING, MARYLAND

Ms. POTRZEBOWSKI. Thank you. Good morning, Mr. Chairman, Mr. Becerra, and Members of the Subcommittee. My name is Patricia Potrzebowski, and I serve as Executive Director of the National Association for Public Health Statistics and Information Systems, or NAPHSIS.

NAPHSIS represents the 57 jurisdictions responsible for vital records in the United States, including the 50 States, the District of Columbia, New York City, and the 5 territories. I am pleased to offer this testimony on the important civil registration function of vital records, and more specifically, enhancements the vital records jurisdictions are making to improve the accuracy, security, and timeliness of death registration.

Vital records are permanent legal documents, and include live births, deaths, fetal deaths, marriages, and divorces. The 57 vital records jurisdictions, not the Federal Government, have legal authority for the registration of these vital events. As such, the records themselves, how they are collected, with whom they may be shared, and how they may be used are governed by State laws. The Federal Government does not maintain a national database that contains all of this information.

Many organizations and millions of Americans use vital records or certified copies of them for legal, health, personal, and other purposes. Birth certificates are used to obtain official IDs, such as driver's licenses and passports, as well as for school entry and qualifying for State and Federal benefits. Death certificates are used to collect life insurance, stop benefit payments, and settle estates.

The information contained on birth and death certificates comes from a variety of sources. For birth, these are primarily hospitals and the mothers of newborns. Funeral directors are generally responsible for completing death certificates, based on information

supplied by next of kin. Physicians, medical examiners, or coroners certify the cause and manner of death.

After data providers submit these data, the vital records jurisdictions then review process and officially register the event. The jurisdictions maintain the official registries of vital events, and issue certified copies of birth and death records. The jurisdictions also provide the Federal Government with selected vital records data to compile national health statistics, to facilitate secure Social Security number issuance for newborns, and to report individuals' deaths.

Paper-based death certificate systems contribute to inaccuracies and delay data availability. In such systems, funeral home staff often hand-deliver records to physicians for signature, which is both time-consuming and costly. Electronic death registration systems, or EDRS, are now replacing manual systems to better meet administrative and public health needs. To date, 37 vital records jurisdictions have implemented an EDRS. A chart showing that EDRS implementation by jurisdiction is included in my written statement.

An EDRS solves many long-standing issues related to accuracy, security, and timeliness of death data. An EDRS includes built-in real-time edits and cross-checks. Automatic reminders and workflow prompts notify the physician by email when a death certificate is ready for electronic signature. This results in more timely registration of the death, as well as faster submission of death records to SSA.

While vital records jurisdictions have made great strides in implementing EDRS, there is still much to be done. Installation of an EDRS in a vital records office is just one part. To be effective, all data providers, especially funeral homes, health care facilities, physicians and coroners must also use the EDRS. Full implementation of EDRS may take years, and involves a significant financial commitment by State health departments. Lack of adequate resources, both financial and human capital, are the biggest barriers to more widespread EDRS adoption.

In the past, SSA provided funding to many vital records jurisdictions to help support their EDRS implementation efforts. NAPHSIS estimates that $20 million is needed to complete EDRS implementation in all 57 vital records jurisdictions, and to increase EDRS use among data providers.

For your consideration, my written statement provides information about another electronic system, the electronic verification of vital events system, or EVVE, that Chairman Johnson mentioned. Developed by NAPHSIS with initial funding from SSA, EVVE is an online system that quickly, reliability, and securely verifies birth and death information in any participating vital records jurisdiction, without the need for a national database.

Several State and Federal agencies, including SSA, are currently using EVVE to verify birth certificate information. EVVE is a significant tool that can be used to verify the authenticity and accuracy of death certificate information.

Thank you for the opportunity to testify. I am happy to address your questions.

[The prepared statement of Ms. Potrzebowski follows:]

Statement for the Record

submitted by

Patricia W. Potrzebowski, Ph.D.

on behalf of

National Association for Public Health Statistics and Information Systems

for

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security

February 2, 2012

Mr. Chairman and Members of the Subcommittee—

The National Association for Public Health Statistics and Information Systems (NAPHSIS) welcomes the opportunity to provide the House Committee on Ways and Means, Subcommittee on Social Security this written statement for the record on vital records and specifically, the reporting and electronic verification of deaths. Established in 1933, NAPHSIS is a non-profit membership organization representing the 57 vital records jurisdictions that collect, process, and issue vital records in the United States, including the 50 states, New York City, the District of Columbia and the five territories. NAPHSIS coordinates and enhances the activities of the vital records jurisdictions by developing standards, promoting consistent policies, working with federal partners, and providing technical assistance.

Vital Records Serve Important Civil Registration Function

Vital records are permanent legal records of life events, including live births, deaths, fetal deaths, marriages, and divorces. Their history in the United States dates back to the first American settlers in the mid-1600s, and in England as early as 1538.[1] More than 8 million vital events were recorded in the United State in 2009.[2]

Many organizations and millions of Americans use these records—or certified copies of them—for myriad legal, health, personal, and other purposes.

- Birth certificates provide proof of birth, age, parentage, birthplace, and citizenship, and are used extensively for employment purposes, school entrance, voter registration, and obtaining federal and state benefits (e.g., Social Security). Birth certificates are the cornerstone for proving identity, and as breeder documents are thus used to obtain other official identification documents, such as driver licenses, Social Security cards, and passports.

- Death certificates provide proof of date of death, date and place of internment, cause and manner of death, and are used to obtain insurance benefits and cease direct benefit payments, transfer property, and generally settle estates.

Data providers—for example, hospitals for birth information and funeral homes, physicians, and coroners for death information—submit birth and death data to the vital

[1] *U.S. Vital Statistics System: Major Activities and Developments, 1950 – 1995.* Centers for Disease Control and Prevention, National Center for Health Statistics. Feb 1997. Available online at: http://www.cdc.gov/nchs/data/misc/usvss.pdf

[2] National Center for Health Statistics, Centers for Disease Control and Prevention. Available online at http://www.cdc.gov/nchs/data/databriefs/db16.htm and http://www.cdc.gov/nchs/data/nvsr/nvsr58/nvsr58_25.pdf

records jurisdictions so that the vital event can be reviewed, edited, processed and officially registered. The jurisdictions are then responsible for maintaining registries of such vital events and for issuing certified copies of birth and death records.

The federal government does not maintain a national database that contains all of this information. Consistent with the constitutional framework set forth by our founding fathers in 1785, states were assigned certain powers. The 57 vital records jurisdictions, not the federal government, have legal authority for the registration of these records, which are thus governed under state laws. The laws governing what information may be shared, with whom, and under what circumstances varies by jurisdiction. In most jurisdictions, access to death records is restricted to family members for personal or property rights, to government agencies in pursuit of their official duties, or for research purposes. In other jurisdictions, release of death record information may be subject to less restrictive limitations; and in a few states identifiable information from death certificates is publicly available.

In an example of effective federalism, the vital records jurisdictions provide the federal government with data collected through birth and death records to compile national health statistics, facilitate secure Social Security number (SSN) issuance to newborns through the Enumeration at Birth (EAB) Program, and report individuals' deaths.[3, 4] For example, the National Center for Health Statistics obtains de-identified vital events data from the jurisdictions to compile national data on births, deaths, marriages, divorces, and fetal deaths. These data are used to monitor leading causes of death and our nation's overall health status, develop programs to improve public health, and evaluate the effectiveness of those interventions. In addition, the jurisdictions provide SSA with fact of death information—including the decedent's name, date of birth, date of death, and SSN as filed with the jurisdiction—for use in the administration of the programs established under the Social Security Act to reduce erroneous payments to deceased persons receiving Social Security benefits.

Electronic Systems Enhance Death Reporting Accuracy, Timeliness, and Security

A death certificate contains both demographic (personal) information and medical (cause of death) information about the decedent. Over the last century in the United States, death certificate completion has mostly been the responsibility of funeral

[3] The National Center for Health Statistics, Centers for Disease Control and Prevention, Department of Health and Human Services purchases de-identified data from the vital records jurisdictions through the Vital Statistics Cooperative Program to produce national vital statistics and for research purposes as part of the National Death Index.

[4] The EAB program allows parents to complete applications for SSNs for their newborns as part of the hospital birth registration process. About 96 percent of SSNs for infants are assigned through the EAB process.

directors, with physicians, medical examiners, and coroners providing cause and manner of death information. Once the demographic data and medical data are complete, the death certificate is then filed with the vital records office. In some states, the death certificate is filed at the local vital records office, and then sent to the state office; in other states the death certificate is filed directly with the state office. The data are then reported to state and federal entities for public health and administrative purposes.

Manual certificate preparation, including the personal delivery of records to physicians for signature, extensive and costly travel by funeral director staff to file certificates, and labor-intensive processing of paper records locally and at the state vital records offices, all contribute to slowing registration and delaying the availability of death data.

Furthermore, even though each state has laws requiring the registration of death records within a specific time period, a significant number of certificates are not appropriately filed, may contain incorrect or inconsistent entries, or are not finalized until many weeks after the death occurred. In addition, incomplete death certificates and coroner cases may take weeks or even months to resolve. These late-filed and/or partially completed death certificates are not generally acceptable for use by family members, nor do they meet federal administrative needs or satisfy the information demands of local, state and federal agencies.

In January 1997, the report, *Toward an Electronic Death Registration System in the United States: Report of the Steering Committee to Reengineer the Death Registration Process* was prepared by a task force of representatives from federal agencies—the National Center for Health Statistics and SSA—as well as NAPHSIS and other professional organizations representing funeral directors, physicians, medical examiners, coroners, hospitals, and medical records professionals. The Committee examined in detail the feasibility of developing electronic death registration in the United States. The conclusion of the report was that the introduction of automated registration processes in the states is a viable means to resolve several historical and continuing problems in the process of death registration.

The advent of technology has facilitated the automation of death registration and reporting, which is the key to addressing these long-standing issues related to accuracy, security, and timeliness of data. To date, 37 vital records jurisdictions have implemented electronic death registration systems (EDRS) to better meet the public health and administrative death information needs (see Appendix 1). For states using an EDRS, death reporting is:

- More Accurate and Complete. An EDRS ensures that all required fields are completed before the death certificate is filed using built-in, real-time edits and crosschecks on the data entered. For example, it can ensure that the individual recording the data does not inadvertently indicate that a two-year old decedent has a college education. For purposes of SSA, an EDRS incorporates a real-time check of

the decedent's SSN against the SSA data files to ensure accuracy of the SSN recorded before the death certificate is registered and filed.[5]

- More Timely. An EDRS allows different death data providers, e.g. the funeral director and physician, to complete the death record concurrently from their computers. It eliminates the need for a paper death certificate to be hand-delivered by funeral home staff to the physician's office for completion. Automatic reminders and workflow prompts are built into an EDRS so a physician is notified via e-mail when a death certificate is awaiting completion. Once the electronic death record is complete, state vital records offices may submit fact-of-death records to SSA daily (Monday-Friday).

- More Secure. An EDRS requires a distinct username and password for each death data provider to access the death records. An EDRS also has built-in audit trails to monitor the users' activity.

While vital records jurisdictions have made great strides in implementing EDRS, there is still much to be done. In some of the 37 vital records jurisdictions that have implemented EDRS, not all physicians or funeral directors submit death records electronically. Implementation of the EDRS in the vital records office is just one piece of the puzzle. To be effective, all data providers—funeral homes, hospitals, physician offices, nursing homes, hospices, coroners and medical examiners —also must use the system. These users must then adjust their workflow processes and make themselves available for training. From start to finish, the full rollout of an EDRS may take years and a significant financial commitment on the part of the state and local health departments and the death data providers themselves. The lack of adequate resources—both financial and human capital—are the biggest barriers to more widespread EDRS adoption. This is particularly true for death data providers who do not report a significant number of deaths each year, and therefore do not see the value of the required investments.

Between 2001 and 2006, SSA provided funding to many vital records jurisdictions to help support their EDRS implementation efforts. Based on a late-2008 survey of the vital records jurisdiction, NAPHSIS estimates that $20 million is needed to complete EDRS implementation in all 57 vital records jurisdictions and to increase use of EDRS among death data providers. Some additional funding may be required on an annual basis to facilitate death data provider training.

[5] Among the 37 vital records jurisdictions with EDRS, three have not integrated the capability to verify SSN into their EDRS: Illinois, Maine, and Wyoming.

Preventing Fraud, Identity Theft through Electronic Verification of Vital Events (EVVE)

Because vital records are essential legal documents linked to identity, and because criminals need new identities, vital records are sought out and used to commit fraud, identity theft, and even terrorist activities.[6, 7, 8] It is therefore essential that birth and death records be protected, and that federal and state agencies have the ability to verify the source data contained therein. In addition, the ability to quickly catch and stop the fraudulent use of Social Security and other public benefits would reduce wasteful spending, and restore public trust in government.

Recognizing the need to verify benefit eligibility in a timely and secure fashion, SSA awarded NAPHSIS a grant in 2001 to develop and implement the Electronic Verification of Vital Events (EVVE) system. EVVE is an online system that verifies birth and death certificate information. It provides authorized users at participating agencies with a single interface to quickly, reliably, and securely validate birth and death information at any vital records jurisdiction in the country, circumventing the need for a national database of such information. In so doing, *no additional personal information is divulged* to the person verifying information—EVVE simply relays a message that there was, or was not a match, with the birth and death records maintained by the state, city, or territory. In addition, EVVE has the capability to flag individuals who are deceased, eliminating a key loophole whereby thieves use a valid birth certificate of a deceased individual to create a new identity.

Today, SSA uses EVVE to verify proof of age and place of birth as a program policy requirement before issuing Social Security benefits. EVVE is used by other federal and state agencies to verify or certify identification and authenticity of birth certificates:

- Passport Fraud Prevention Managers began using the EVVE system in March 2009 for birth certificate verifications. In their first six weeks of use, there were two instances where the Fraud Prevention Mangers used the EVVE system to electronically verify the birth certificates, and EVVE returned a 'no match.' Upon further follow up with the vital records offices that 'issued' the birth certificates it was determined that indeed the birth certificates presented with those passport applications were fraudulent. Based on these and other successes, NAPHSIS is

[6] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States, July 2004, p. 390.

[7] Department of Health and Human Services, Office of Inspector General, *Birth Certificate Fraud*, Sept. 2009 (OEI-07-99-00570).

[8] Government Accountability Office, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process,* Mar. 2009 (GAO-09-447) and *State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud*, July 2010 (GAO-10-922T)

working with the Department of State to integrate EVVE into the standard passport adjudication process.

- The Office of Personnel Management (OPM) is responsible for processing federal employment applications and at times security clearances. To reduce the administrative burden of applicants submitting certified birth certificates, OPM uses EVVE to electronically certify an individual's citizenship in lieu of obtaining a paper copy of the birth certificate. OPM conducted a pilot in parallel with their manual voucher process of requesting certification information from the vital records jurisdictions. The match rate for those same queries was 84 percent in both manual and EVVE mode. In addition, the response time was just 10 seconds using EVVE compared to 42 days using the manual process.

- The Deficit Reduction Act of 2005 requires the verification of citizenship and identity for enrollment in Medicaid through a birth certificate or other official document. The South Dakota Medicaid Office was the first to use EVVE for this purpose in 2007, followed by Medicaid Offices in Mississippi, Minnesota, and Washington, as well as the Mississippi Health District Offices. Since then, several other states have inquired about using EVVE for determining Medicaid eligibility.

- In response to the 9/11 Commission's recommendations for secure identification documents, Congress enacted the REAL ID Act in May 2005, requiring that driver's license applicants present their birth certificates to the Department of Motor Vehicles (DMV) to validate U.S. citizenship and date of birth, and that DMVs verify the authenticity of those birth certificates using EVVE. Three state DMVs—North Dakota, South Dakota, and Iowa—used EVVE in this capacity as part of a federally-funding pilot program through the Department of Homeland Security.

These users are enthusiastic about the EVVE system, citing its ability to:

- Provide protection against the potential use of birth certificates for fraudulent activities.

- Improve customer service by facilitating rapid access to accurate and verifiable vital record data in real-time.

- Safeguard the confidentiality of birth and death data.

- Offer a secure mechanism for communication between agencies and vital records offices via the Internet.

- Easily integrate with current legacy systems that the federal or state agencies may already be using, and for serving as a user-friendly interface for agencies that seek a stand-alone query system.

In April 2011, the Office of the National Coordinator for Health Information Technology, HIT Policy Committee Enrollment Workgroup Committee recommended the use of EVVE as a potential tool to facilitate enrollment in federal and state health and human services programs, such as offerings by new health insurance exchanges established through the Affordable Care Act.

As of February 1, 2012, EVVE is currently installed in 36 vital records jurisdictions (see Appendix 1). NAPHSIS is working to install EVVE in the remaining 21 jurisdictions, with 11 jurisdictions currently in progress. NAPHSIS has also procured a data analysis and quality control tool that all jurisdictions can utilize to analyze their EVVE database for anomalies, inconsistencies, accuracy, and completeness. This tool and the analysis of EVVE data has been completed in 30 jurisdictions, as of February 1, 2012.[9]

Despite EVVE's security, speed, and ease of use, the system is only as good as the underlying data infrastructure upon which it relies. Digitizing paper-based birth and death records, then cleaning and linking those records, will provide for secure, reliable, real-time identity verification using EVVE. For example, there are cases where an individual has assumed a false identity by obtaining a birth certificate of a person who has died. Therefore, it is important that all jurisdictions' death and birth records be linked to flag individuals who are deceased and identify fraudulent birth documentation.

The vital records jurisdictions' efforts to digitize, clean, and link vital records have been hindered by state budget shortfalls. In short, the jurisdictions need the federal government's help to complete building a secure data infrastructure. Specifically, resources are needed to help vital records jurisdictions digitize their birth records back to 1945, to clean these data to support electronic queries, and link birth and death records.

NAPHSIS appreciates the opportunity to submit this statement for the record and looks forward to working with the Subcommittee. If you have questions about this statement, please do not hesitate to contact NAPHSIS Executive Director, Patricia Potrzebowski, Ph.D., at ppotrzebowski@naphsis.org or (301) 563-6001. You may also contact our Washington representative, Emily Holubowich, at eholubowich@dc-crd.com or (202) 484-1100.

[9] Potential EVVE users interested in obtaining additional information about applying to become an approved EVVE user for either verification or certification of vital events should contact Rose Trasatti Heim via email at rtrasatti@naphsis.org.

Appendix 1: Status of Electronic Death Registration System (EDRS) and Electronic Verification of Vital Events (EVVE) System, by Vital Records Jurisdiction[i]

Jurisdiction	EDRS[ii]	EVVE[iii]
Alabama	✓	✓
Alaska		
American Samoa		
Arizona	✓	✓
Arkansas	✓	✓
California	✓	✓
Colorado		✓
Connecticut	✓	✓
Delaware	✓	✓
District of Columbia	✓	✓
Florida	✓	
Georgia	✓	✓
Guam		✓
Hawaii	✓	✓
Idaho	✓	
Illinois	✓	
Indiana	✓	✓
Iowa		✓
Kansas	✓	✓
Kentucky	✓	✓
Louisiana		✓
Maine	✓	
Maryland		✓
Massachusetts		
Michigan	✓	✓
Minnesota	✓	✓
Mississippi		✓
Missouri	✓	✓
Montana	✓	✓
Nebraska	✓	✓
Nevada	✓	
New Hampshire	✓	
New Jersey	✓	✓
New Mexico	✓	
New York City	✓	✓
New York State		
North Carolina		
North Dakota	✓	✓

Jurisdiction	EDRS	EVVE
Northern Marianas		✓
Ohio	✓	✓
Oklahoma	✓	✓
Oregon	✓	✓
Pennsylvania		✓
Puerto Rico		
Rhode Island		✓
South Carolina	✓	
South Dakota	✓	✓
Tennessee		
Texas	✓	
Utah	✓	✓
Vermont	✓	✓
Virgin Islands		
Virginia		
Washington	✓	
West Virginia		✓
Wisconsin		
Wyoming	✓	
Total	**37**	**36**

[i] Implementation status as of February 1, 2012.

[ii] This column indicates in which jurisdictions the vital records office has adopted an EDRS. It does not indicate total penetrance of EDRS among death data providers in that jurisdiction. The implementation of EDRS if in progress in three vital records jurisdictions, including Louisiana, Mississippi, and Wisconsin. Ten jurisdictions are in the planning stages, including Alaska, Colorado, Iowa, Maryland, Massachusetts, New York State, North Carolina, Pennsylvania, Tennessee, and Virginia.

[iii] As of February 1, 2012, the implementation of EVVE is also in progress in 11 vital records jurisdictions, including Alaska, Florida, Massachusetts, Nevada, New Mexico, North Carolina, South Carolina, Tennessee, U.S. Virgin Islands, Virginia, and Wyoming.

Chairman JOHNSON. Thank you, ma'am. You know, Mr. Pratt recommended we change the law to codify certain business access to the Death Master File, including State records. Can you tell Mr. Pratt the history of the powers assigned to the States and their legal authority?

Ms. POTRZEBOWSKI. Well, I am certainly not a constitutional lawyer, Mr. Chairman.

Chairman JOHNSON. No, but you do understand that. And what is the legal authority regarding vital records concerning the States?

Ms. POTRZEBOWSKI. Right. So the States have the legal authority, because it is not mentioned in the Constitution. So that is clearly the States' authority, to set the rules for registering the vital events, for determining how the data shall be used, the confidentiality of the information, and the sharing of that information with whomever they wish.

Chairman JOHNSON. Yes. So each State is different, is it not?

Ms. POTRZEBOWSKI. And every State is different. You know how that works.

Chairman JOHNSON. Yes. And they probably have different records, too.

Ms. POTRZEBOWSKI. Unfortunately, there is a little bit of variation. Most of the States have a general basic data set that they follow.

Chairman JOHNSON. Mr. Agin, how did you connect the theft of your daughter's Social Security number to the Death Master File?

Mr. AGIN. I mean this is my personal belief, based upon my research and based upon our discussions with other families.

When the information is so readily available to anybody with a computer, there is only several manners in which somebody could have found, number one, that my child died—we do maintain a blog, so anybody who is following along, or people, I believe, troll these blogs to see how children are doing, could have connected the dots. And then I believe that people know that that information is readily available on these genealogical websites. So I think that that connects the dots, in terms of the readily available information.

The only other possible explanation for obtaining her Social Security number could be somebody at one of the institutions where she was treated that maintain her medical records. But, you know, I would like to believe that that is not the case.

Chairman JOHNSON. No, I kind of agree with you on that.

You have heard the testimony of the other witnesses. Is there any reason that Social Security, the Commerce Department, or any Federal agency, for that matter, ought to be disclosing private death information to the general public?

Mr. AGIN. To the general public? In my opinion, no. I think that the Death Master File does have its obvious stated purposes, which include foreclosing fraud, as Mr. Pratt discussed. And I think that is a vital use of the Death Master File.

I think that the publication of the Death Master File in the manner in which we do it today is serving identity thefts with this type of information on a silver platter. There are several ways to try to

go about foreclosing that: withhold individuals recently deceased for a period of time, disclose only a handful, the last four digits of the Social Security numbers. There is a number of manners and methods that I think would satisfy all the communities involved that use the Death Master File.

So, as it stands, does somebody need my daughter's full Social Security number, date of birth, date of death, full address, and her zip code? Absolutely not.

Chairman JOHNSON. I hear you. Thank you for your testimony.

Mr. AGIN. Thank you, Mr. Chairman.

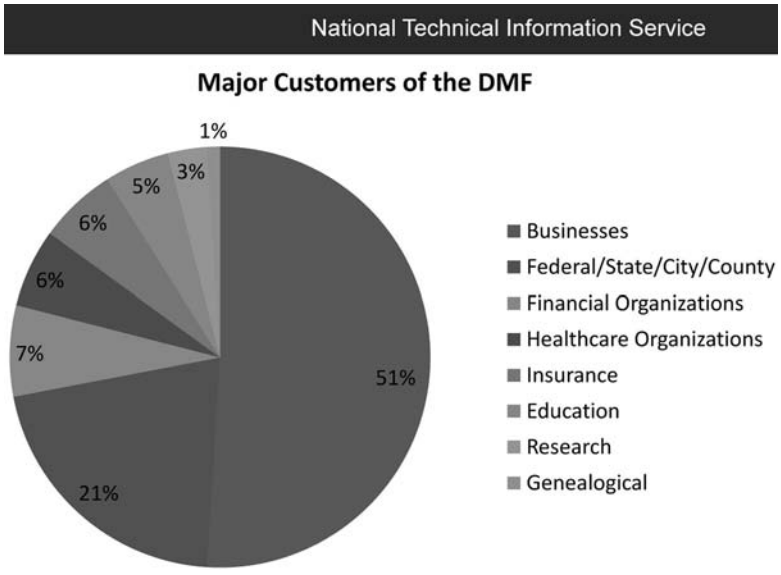
Chairman JOHNSON. Mr. Becerra, you are recognized.

Mr. BECERRA. Thank you, Mr. Chairman. Mr. Agin, first I would like to begin with you and ask, because you have gone through this, it seems to me that our biggest issue is going to be in trying to convince a lot of the private sector entities that use this information that they have to covet the information once they get it.

You—I would assume you believe that some of these private sector businesses need to get accurate information so that they can make sure that people don't receive benefits, income that they are no longer eligible for, because someone has died, is deceased. But how do you constrain the use of the information?

And I am looking at this chart. I wouldn't have guessed this. It shows the major customers for the Death Master File. We talked about those who help determine our genealogy. One percent. They constitute 1 percent of the customers who purchase this Death Master File information, your daughter's information. The biggest customers for all those bits of data? Businesses. Then you have the Federal, State, city, county governments, financial organizations, health care organizations, insurance, education, research. And, at the end, genealogical.

[Insert of The Honorable Xavier Becerra follows:]



And so, I would imagine Mr. Pratt would say, "This is valuable information that helps us avoid fraud from the other side." And so, is there something that you—and you mentioned legislation that you are supportive of. Some people think that it is a little too narrow in its scope. And Mr. Pratt suggested, I think, some possible ways to address that.

Mr.—is it Breyault?

Mr. BREYAULT. Breyault, yes.

Mr. BECERRA. Mr. Breyault also suggested some potential changes.

Having heard your testimony, do you agree with what they have said could be a good way forward to try to have legislation that avoids the situation you and your wife faced?

Mr. AGIN. Thank you, Mr. Becerra. Absolutely. I think there is no question of balance that can be struck with respect to the lawful stated purposes for the use of the Death Master File.

As a parent who has gone through this, I am not interested in foreclosing the use of the Death Master File to go after other fraudulent uses and the financial institutions in the business sector who rely upon that data in ensuring that their claims are managed properly, that they are paying the right individuals, that they are not paying the wrong individuals.

Again, I think there are a number of ways to do that: stiffer penalties, registration for anybody who is interested in purchasing the information, certifying that they will not use it for widespread distribution.

With respect to the chart that you showed, regardless of whether or not the genealogical services only make up 1 percent of the purchasers, they are still the individuals who are putting it out for free on their websites. So anybody sitting in this room with a computer can find my daughter's Social Security number. Anybody can find any of your relatives who have passed away. They can find their Social Security numbers.

Mr. BECERRA. Good point.

Mr. AGIN. So, regardless of the amount on that pie chart, I would submit to you that that is the largest factor for the commission of this type of fraud against individuals in my community.

So, I am very interested to strike a balance so that the lawful use of this information is not foreclosed.

Mr. BECERRA. And, Mr. Chairman, to me, when we passed that bipartisan bill out of this Committee a while ago dealing with identity theft—actually dealing with those who are still living—we ran into a brick wall with the Financial Services Committee, because so many financial services companies were very concerned that we would close the door to their access to information they believe they need. And before you knew it, the bill was dead.

Mr. Pratt, my sense is that there are going to be a lot of folks out there in the business community who legitimately make use of this, including the folks who do genealogical studies, who say, "Wait a minute, you know, this information is out there." What do we do to make sure that we address the legitimate concerns of those in the private sector that need this information, but still constrain its use?

I happen to agree with Mr. Agin, that I think you have—and, Mr. Chairman, I would say that I think you have to act with a swift and stiff penalty against anyone who abuses this information. And I would love to have someone, some entity, be the poster child of what happens to you if you take Mr. Agin's daughter's information and use it the wrong way.

Mr. PRATT. Again, I think we are starting to move down into the details of exactly how you accomplish—I think the big goal—there seems to be a lot of agreement on the large goal. There is a difference between the problem we have, which is, because of FOIA, the Social Security Administration, through Commerce, is disclosing the record to anybody. And some are making it available in a very public way, so that there is no process on the front end to evaluate why I want to have access to that record.

We are somewhere else on that pie chart that you held up. And that is why we feel very confident that there is a way to draw a distinction between, yes, I understand there may be some process by which we have to validate who we are and why we need the information for those reasons, and to stipulate those reasons. We live with some of that in the data world, always. And we are happy to work in that context, to try to find a way forward.

You are absolutely right. We need the information. We need the full Social. We have done studies where common names, amazingly enough, you can find two different Smiths with the same last four digits of a Social. And because a Death Master File annotation is a big event—you either are dead or you are not; consumers generally don't appreciate being declared deceased when they are not—we really feel a full Social is important.

But we are happy to live—like I said before, we live in a contract world, we live in a data security world. We live in a business-to-business context. We want to stop fraud. That is the motivation for doing this. There is no other business model we are trying to build that sort of colors outside those lines. I am really confident that there is a way to get this done. And it is different than perhaps the debate that we went through last time.

Mr. BECERRA. Yes, I think it is. I appreciate your words.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you for your questions. Mr. Marchant, you are recognized.

Mr. MARCHANT. Thank you, Mr. Chairman. Mr. Breyault, is that the way you say it?

Mr. BREYAULT. Yes, that is correct, sir.

Mr. MARCHANT. I thought I heard you say that 10.2 percent of children have had their identity compromised in some way.

Mr. BREYAULT. They have had their Social Security number misused by someone else.

Mr. MARCHANT. Okay. Do you have that from a study?

Mr. BREYAULT. Yes, sir. It is from Carnegie Mellon University. It is a researcher by the name of Richard Power. The full citation is in my written statement, sir.

Mr. MARCHANT. Okay. Well, thank you very much. For that—Mr. O'Carroll, for that small group of people, or children that for some reason have not gotten an assigned Social Security number,

how do they appear, when they pass away, on the Death Master File? Or do they not appear?

Mr. O'CARROLL. What will happen is with the State match, the State is going to match against Social Security numbers. And if the child wasn't issued a Social Security number, that wouldn't then be part of the Death Master File for SSA, since they weren't recognized with an SSN yet on that one. So that is part of the matching process that we do.

But as you said before, in the case of your grandchildren, virtually every child now is, at the time of birth, being enumerated. And it is an extremely rare occasion that a child wouldn't be enumerated.

Mr. MARCHANT. So any parent that found themselves in the same situation as Mr. Agin, there would not be a situation where they could protect themselves—probably because of your health benefits, enrolling them in a health care plan, you would have to get that information?

Mr. O'CARROLL. The enumeration of birth has been a process with Social Security now for a number of years. It has been accepted by most of the medical institutions, and it is a very effective way of enumerating people. What was happening in the past was, within the first year for tax purposes or whatever, the parents were coming in for a Social Security number. So, by doing it this way, it is a more controlled way and effective way of doing it.

So, there really isn't an opt-out, at least to my knowledge. I am sure you could, but it is very, very rare that anybody has.

Mr. MARCHANT. Well, I think that parents find themselves in the situation where this information is out there. I think it is vital that we move quickly on this. I do understand the—I think we will find—I think this Committee will find very quickly that that 1 percent group that is on that chart will begin to be very vocal, and we need to make sure that they understand the difficulty that we are dealing with.

We faced a similar problem at the—when I was in the State legislature about the release of vital information. And we experienced a—it was a—quite a fight to ultimately strike the balance between these groups. But I am committed to do it.

Mr. Chairman, I appreciate you bringing this issue to the forefront, and committed to help you with it.

Chairman JOHNSON. Thank you, Mr. Marchant.

Let me ask one more question, Mr. Pratt. The Death Master File has always been an incomplete record of deaths, as Social Security will admit. The Death Master File may be a starting point for death databases, but you have to confirm the data. What are your other sources of death data?

Mr. PRATT. For example, in the case of credit reporting, when an individual passes away, then the trustee or the executor of the estate will likely begin to notify financial institutions in order to pay out that last bill. And those financial institutions will report that data back into the credit reporting system, as well.

But it is an incomplete system. Our concern here, of course, is losing the Death Master File removes just another critical component, and we are more blind than we otherwise would be. It is true,

there are going to be times where we will still, in this country, not know that somebody is deceased until much——

Chairman JOHNSON. Aren't you able to get the death data from the State?

Mr. PRATT. States are—you know, it is a very disintermediated process. It is very hard to go out and gather that information on a State-by-State basis. There are—we have even heard here testimony about new technologies that may be making that easier on a go-forward basis. Some of these technologies appear to be look-up—in other words, a record-by-record, rather than bulk types of delivery technologies.

And so, Mr. Chairman, there may be ways, going forward, to improve and build on what we have today. We are just trying to preserve what we have today.

Chairman JOHNSON. Well, you, I am sure, are willing to pay something for it. What price do you think Mr. Agin would put on his daughter's Social Security number?

Mr. PRATT. Yes, I don't think there is any price. I am a parent myself, and I have had a number of my board members who are parents call me directly about this very same thing, Mr. Chairman. We all are focused on trying to find the right way forward.

Chairman JOHNSON. Okay. Well, we are going to work on it, and Mr. Becerra has agreed to help me. And we will do that.

I thank you all for being here today, and for your testimony. We do need to act now to stop thieves from exploiting our deceased loved ones. And, Mr. Becerra, I look forward to working with you on this issue.

With that, I thank you all for being here; the Committee stands adjourned.

[Whereupon, at 10:23 a.m., the Subcommittee was adjourned.]

[Questions for the Record follow:]

Enclosure – Questions for the Record – February 2, 2012 Hearing

1. **It has been suggested that your current notification policy (related to someone's Social Security number being made public by mistake) violates the Privacy Act and the Office of Management and Budget's guidance. What is your response?**

   OMB guidance (M-07-16) provides that an agency should notify individuals when there is a reasonable risk of harm, but should avoid creating unnecessary concern or confusion when the risk level is low. We do not notify an individual unless we identify misuse. If we find a case of misuse, we will notify the affected individual immediately and offer credit monitoring or other appropriate identity theft protection services. However, since 2008 when we began reviewing persons erroneously listed on the DMF to look for patterns of misuse, we have not identified any cases of misuse.

   We are reviewing our policy to determine whether it strikes the right balance and is respectful of public perception. We expect to complete our review in 90-120 days. Not having to release death information to the public would largely resolve this issue with regard to the Death Master File.

2. **Your Inspector General has criticized the agency for not notifying the 14,000 living people who are erroneously put on the Death Master File (DMF) each year. I understand the Social Security Administration (SSA) has a contractor review these cases for patterns of possible misuse. Would you tell us more about that process? How much time does it take for the SSA to discover and remove the errors for those living from the DMF? If there are patterns of misuse would you then notify the individual directly? You mentioned during the hearing that you were reviewing your notification policy. When can we expect the results of your review?**

   We contract with ID Analytics, a leading identity risk management firm, to review the cases in which we have erroneously placed a living person on the DMF. ID Analytics operates the ID Network, a cross-industry collaboration of data sharing for the purpose of identity fraud prevention. ID Analytics examines risk events, primarily new account opening or account changes, for the likelihood that these events represent identity fraud. ID Analytics reviews these cases quarterly for a period of three years. To date, it has not identified any patterns of misuse. If it were to identify misuse, we would promptly notify individuals and offer credit monitoring.

   While we do not track how long it takes to identify an error on the DMF, we act quickly to correct an error when we discover it. We expect to complete our review in 90-120 days and will share the results with you.

3. I understand the SSA offers a consent-based SSN verification system that includes death information. Would you tell us more about this system and your views regarding whether it could be a source for death information should Congress change the law to prevent the Death Master File from being made public?

Private companies and Federal, State, and local agencies pay to use our Consent Based Social Security Number Verification Service (CBSV) to verify Social Security numbers (SSN). In order to use CBSV, entities must have a properly signed consent form, and they may only use the verification results for the reason the client specifies.

CBSV verifies whether a name/SSN combination matches data in our records. Each name/SSN combination submitted to CBSV is returned with a "yes" or "no" verification code, which indicates that the submission either does or does not match our records. If the name/SSN match and our records show that the SSN holder is deceased, the response includes the fact of death but not the date of death.

We do not believe CBSV would be a satisfactory alternative to the DMF in most cases. Unlike the DMF, CBSV requires the consent of the Social Security number holder and provides only an indication of death, not the information most users want, such as date of death. In addition, CBSV is a one-time verification process. Users enter one name/SSN combination at a time. In contrast, the DMF is a database of death information, which can be run against the purchaser's own records.

4. Under the Social Security Act, the SSA may give states death data to administer benefits "wholly funded by the state." In the case of state retirement benefits, the employees help fund the pension through their contributions. Since state retirement benefits are not "wholly" funded by the State, state benefit retirement agencies must obtain death records to administer their programs by purchasing the Death Master File. I don't think this was the intent of the law. What is your opinion?

Section 205(r)(3) of the Social Security Act provides that we may share our death information with Federal and State agencies to ensure proper payment of federally-funded benefits, while section 205(r)(4) states that we may provide our death information to States for their use in programs only if those programs are wholly funded by the States. By including "wholly," Congress left no discretion to share the full DMF with State agencies to administer programs that are funded by employees as well as State governments.

However, State retirement systems should be able to get State deaths from their State department of vital records.

5. Would you explain your policy of issuing new Social Security numbers (SSNs) to children whose identities have been compromised? Children usually have no wages so why not respect a parent's wishes to protect their child? How do you know that the number won't be used in the future for some harmful purpose? Does your agency at least flag the number as stolen in your verification processes?

In light of the increase in identity theft, we are currently reviewing our policy to ensure it is responsive, especially to children.

Our current SSN policy tries to balance appropriate and necessary control over the issuance of SSNs with the need to address unique events that warrant a new number. We assign a new SSN when a person provides evidence that criminal or harmful misuse of the number has caused recent economic or personal hardship. We also advise the person that a new number may not solve all problems. Because of the widespread use of the SSN, the person may have difficulty transitioning to the new number with employers, banks, credit bureaus, and other entities. Even the SSNs of children who have no earnings may have already been shared with many entities, beginning with pediatricians and health insurance providers.

Once we assign a new number, we refer the person to the Federal Trade Commission to request a fraud alert be placed on credit records. We also flag the old number in our records. Employers, State agencies issuing driver's licenses and identification cards, and CBSV users see this flag when they use our verification routines.

6. Has the National Association for Public Health Statistics and Information Systems participated in the interagency working group? Further, when you contract with states for their death data, what kind of agreements are there? Please indicate the general terms of these agreements. Are all state agreements similar? Are there restrictions on the use and sharing of this data to other parties including other federal agencies?

To our knowledge, the National Association for Public Health Statistics and Information Systems has not participated in the OMB-led review of the policy behind the availability of death information.

Our contractual agreements with the States to provide death information are based on the provisions of section 205(r) of the Social Security Act. These agreements outline the data we can exchange and its permissible uses, including rules for sharing the data. Each State contract contains the same language, regardless of whether the State participates in Electronic Death Registration (EDR), an initiative to automate the paperbound death registration process.

Section 205(r) prohibits us from redisclosing death information provided to us by the States, except to Federal and State agencies that provide federally-funded benefits and States that administer benefit programs wholly funded by the State. Additionally, the law provides us with discretion to provide death information to Federal and State agencies for research and statistical purposes.

We have attached a blank copy of a State contract for your information.

7. **Social Security shares the death information in its internal databases with other agencies that also provide benefits, such as the Department of Veterans Affairs (VA). Do these agencies make this information available to the public? Do your data sharing agreements prevent these agencies sharing this information publically or with any other agency?**

   We share death information with Federal benefit-paying agencies following the computer matching and privacy protection requirements of the Privacy Act. These agreements prohibit agencies from redisclosing the data we send them.

8. **What would it cost to bring all remaining non-participating states into the Electronic Death Registration system?**

   We defer to the Department of Health and Human Services (HHS) with respect to the costs involved in the development of EDR systems.

9. **In considering potential solutions as to how we ensure that entities using the information contained on the Death Master File are still able to access the data, would there be a way for the SSA to work directly with the entities that have a need for the Death Master File to receive the information directly from Social Security rather than through a third party?**

   OMB has been working with us and the Departments of Treasury, Justice, and Defense to craft a legislative approach to limit the public availability of death information. The Administration has previously presented the specifications for a draft bill to Committee staff, and will soon formally submit that draft bill for the consideration of the Congress, which reflects our preferred balance between protection of personally identifying information (PII) and allowance of limited access with strict accountability. We look forward to working with the Committee on that draft bill. Please note that there is no benefit to SSA to share this information. We do so because FOIA requires it.

10. **I learned about a North Dakotan who is having a similar issue to some of the one's we've been discussing with the Death Master File. The person was notified for the second time of his wrongly reported death listing by the VA. The incorrect information regarding his death also made it onto the Internet. However, we did receive a notice from the VA about the error. I would like to know, if the VA can catch this kind of error, and then notify the affected individual, do you think the SSA could use a similar process so that the individual can take steps to protect their personal information?**

    We will contact the VA during our notification policy review to learn more about its breach notification processes. We will adopt any cost-effective measures to more quickly identify

errors on the DMF, without relying on self-reports. Early identification of these errors would limit PII exposure and lessen any hardship for affected individuals.

Attachment

Blank State contract

CDIA
CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity

1. If vital statistics constitutionally belong to the States and they guard its privacy very strictly, how would access by private parties keep these two important principles in place? To provide this data to private parties there should be a significant price to compensate the States and heavy penalties for those who break the law. Would your members be willing to pay the States a price close to what you pay other providers for personal data? Of your cost of doing business, purchasing personal data for inclusion in your databases is what percent of the cost of the final product?

A.1 – It is CDIA's long-held view that records obtained by government should be public records and not hidden from view. The following excerpt from a paper[1] authored by Professor Fred H. Cate and Richard J. Varn sets an important context that supports continued open access to state records and to federal records systems including access to the Death Master File (DMF):

"The open public record system has been the mainstay of the U.S. democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports. The American open public record allows citizens to oversee their government, facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."

[1] Fred H. Cate, Richard J. Varn, The Public Record: Information Privacy and Access – A New Framework for Finding Balance, p. 5.

As discussed in our testimony our members' need for the Death Master File (DMF) is set into the context of responsible uses that involve business-to-business transactions. These uses are critical to protecting consumers and contribute to compliance with federal laws and the safety and soundness of the financial services industry. They also include reconnecting consumers with assets that in some cases may be life-changing (e.g., discovering a pension income you didn't know you had or a life insurance policy payment that you did not know about). It is critical that such data be available in an easily accessible and centralize manner to ensure that it is loaded quickly since misuse of a deceased person's data can occur soon after death. In fact just following the national tragedy of 9-11 CDIA was asked to testify as to why DMF data could not be loaded even more quickly to ensure that terrorists, including some involved in this attack on US soil, could not take advantage of US assets such as access to the financial services industry. We do not believe that it is in the best interests of the country to shut down the DMF and assume that a similar system for gathering death records can be created on a state-by-state basis.

Our members' uses of the DMF do not contribute to the terrible problems, particularly those faced by parents who have lost a child, that result from making DMF data accessible to the general public.

State vital records are critical to a full and complete DMF. Where a state asserts its control over such data we would urge them to lift any embargo for the types of purposes enumerated in our testimony and in draft language we have shared with your staff. Where the SSA has the power to do so, it should be directed to make the DMF available and encourage states to lift restrictions that impede our country's ability to address a wide range of risks that are time-sensitive.

2. I understand that to get access to this data, you are willing to undergo some kind of unspecified 'accreditation' process? How would you see accreditation process beginning and in your experience, how long does it take agencies to have this process up and working?

A.2 We assume that the SSA and NTIA therein would adopt a risk-based approach to allowing access to the DMF based on reasonable criteria and direction by the Congress to ensure that access is given. Such access could include a contractual agreement to use the data only for purposes permitted. We assume such a process would not be complex and it should not operate as an artificial barrier to providing access for legitimate uses that protect consumers. In terms of details the SSA and NTIA are in a better position to answer this question.

3. As you know, the Death Master File (DMF) is not totally accurate. The SSA and Commerce make this clear when the file is released. Do you confirm the listings for accuracy? How do you do this and what other sources do you use to confirm the DMF data? Based on your analysis, how accurate or inaccurate is the DMF? How has that accuracy, based against your other death data sources, changed with the removal of the Electronic Death Records (EDRs)?

A.3 Our members employ a variety of proprietary means of ensuring that the correct information is associated with correct record. In terms of details, these practices are treated as confidential trade secrets.

As to accuracy we would only say that the DMF is truly a vital record necessary to business-to-business transactions and that it has been successfully used and there's no basis for shutting down access for these uses which protect consumers (including parents of deceased children) and prevent fraud and terrorist access to services.

Finally, note that if the reported 15,000 errors per year in the DMF's is roughly correct, that amounts to an error rate of 0.5% (based on an annual reporting of 2.8 million records).

4. The National Association for Public Health Statistics and Information Systems runs a query system call Electronic Verification of Vital Events that certifies birth and death information from all fifty states. No information is revealed in the query, thereby protecting all private information. The SSA also runs a consent-based system that is also a query system that confirms private information against the SSA databases? Would either one of these be a possible useful source of information for your members. Speak to the issues in terms of volume, accuracy and costs.

A.4 If, as your question suggests, the Electronic Verification of Vital Events does not provide access to full identifying information then it would be unworkable for our members. Our members cannot be dependent on a third-party technology to interface real-time with our members who are delivering billions credit reports, red flags/fraud prevention technologies and the like instantly across the US economy. Further, our members when operating as consumer reporting agencies as defined by the Fair Credit Reporting Act cannot abjure their direct duty to employ reasonable procedures to ensure maximum possible accuracy of the reports they produce to a third-party technology platform.

With regard to the consent-based system there is no such thing as blanket consent in anticipation of death, and it is not otherwise clear what type of consent could be associated with a death record. The current SSA system is manual and cumbersome and not suitable for how the U.S. economy operates.

Thank you for this opportunity to answer additional questions. CDIA believes that a bill can be enacted this year that shuts down general public access to the DMF, which relieves the SSA of a FOIA duty that requires access by all and which also codifies a duty to provide access for legitimate purposes such as those enumerated in our testimony.

Sincerely,

Stuart K. Pratt
President & CEO

SOCIAL SECURITY
Office of the Inspector General

April 5, 2012

The Honorable Sam Johnson
Chairman, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
B-317 Rayburn House Office Building
Washington, D.C. 20515

Attn: Kim Hildred

Dear Chairman Johnson:

This is in response to your letter dated March 22, 2012, in which you requested information related to the Social Security Administration's (SSA) distribution of death data and personally identifiable information, following your Subcommittee's February 2, 2012 Hearing on Social Security's Death Records. I appreciate the opportunity to provide information related to this critical issue. Below are responses to your specific questions.

1. **The Social Security Administration (SSA) is only required to enter the name, the Social Security number and the date of death on the Death Master File, according to the court settlement. However, the SSA includes other information, including date of birth and zip code. You have recommended that the information not required under settlement be removed. However, the Commissioner says he tried to remove the zip code data, and that only resulted in a *Freedom of Information Act* (FOIA) request to release the data anyway. The Commissioner indicated the SSA Office of the Inspector General (OIG) might be confused on this issue. Can you speak to that remark? Is there any way the agency can remove this data without being in violation of FOIA? Is there the possibility of re-opening the Perholtz decision?**

The consent agreement that established the Death Master File (DMF) required SSA to provide only the decedent's last name, Social Security number (SSN), and date of death. Since that time, SSA expanded DMF information to include the individual's first and middle name, date of birth, residential state and zip code. Effective November 2011, SSA removed the decedent's residential and state zip code information from subsequent DMF publications.

During our audit completed in June 2008, Agency officials explained that SSA expanded the amount of information included in the DMF based on DMF subscriber requests. However, we

could not confirm this because SSA could not provide any documentation to support their assertion.

We recommended that SSA 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. Agency officials stated they would consider implementation of this recommendation.

During our follow-up audit completed in March 2011, SSA officials stated the Agency decided not to implement our previous recommendation at the suggestion of its DMF Task Force. According to SSA officials, DMF Task Force members believed there was a strong likelihood of litigation under FOIA if SSA were to reduce the amount of information on the DMF. At the time of completion of our second review, we were not aware of any attempts by SSA to reduce the amount of information published in the DMF. We are not aware of any FOIA litigation on the subject.

Although we may share a different perspective from the Commissioner on exclusion of data from the DMF that is not mandated for disclosure by the *Perholz* Consent Judgment, I can assure you that we are not confused on this issue. I understand the Commissioner's point to be that while *Perholtz* itself only required certain data to be included in the DMF, the additional information that the Agency voluntarily includes in the DMF is also obtainable under the FOIA; so excluding the information from the DMF is an exercise of questionable value given the likelihood of litigation. We disagree.

We believe that absent a legal requirement to include this additional information in the same public file as other court mandated[1] disclosures of personally identifiable information (PII), such information should not be voluntarily disclosed because doing so, regardless of the possibility of a subsequent FOIA request for the information and related litigation, makes misuse of identities easier for identity thieves. Secondly, there is no guarantee that a FOIA requestor would be guaranteed success in litigating for disclosure of information no longer part of the DMF.

Third, we know from our prior audits that some of the information in the DMF pertains to living individuals. To the extent the DMF erroneously contains identifying information about living individuals permitted to be withheld under FOIA as an unwarranted invasion of personal privacy, the Privacy Act mandates withholding such information. Therefore, at a minimum, there is some degree of uncertainty whether a court would rule in favor of a blanket FOIA request for additional information about all individuals listed in the DMF when the DMF continues to include living individuals. Further, information pertaining to living individuals was clearly not part of the 1980 Consent Judgment. While we recognize that this concern may be alleviated if SSA is able to ensure that all individuals listed in the DMF are in fact deceased, at this point we do not believe this is the case.

Legislation, of course, would render the above noted differences in perspectives on disclosure moot, and is the most viable means of protecting this information.

---

[1] Pursuant to the Perholz Consent Judgment.

In response to the last part of your question, my Counsel tells me that it would be futile to attempt to re-open *Perholtz*, now decades old. Rule 60 of the Federal Rules of Civil Procedure requires action no more than one year after entry of judgment or within a reasonable period of time, depending on the circumstances. Further, even if SSA were successful in amending the Consent Judgment, there is no guarantee that the District Court would modify the Consent Judgment in a way that would restrict access to the DMF, and SSA could be subjected to numerous lawsuits asking for the release of the DMF records under FOIA, which could result in another court order requiring the release of such records.

2. **In your testimony you discuss reports the IG has done on personally identifiable information made available to the public and your recommendations to the SSA to protect that information. Among your recommendations was for the SSA to notify individuals whose information was incorrectly released on the Death Master File. It is my understanding that the SSA does not notify all individuals whose information has been incorrectly released. Could you tell us more about your recommendations and your thoughts on why SSA has not implemented them? I have also asked Mr. Astrue about a situation I recently learned about in North Dakota. This person was notified that his death had been wrongly reported by the Department of Veterans Affairs (VA) and that his personal information has been put on the Internet. The VA caught the error and notified the individual. Could the SSA use a similar process to the VA's to notify affected individuals so they can take steps needed to protect their personal information?**

Our 2008 report included two recommendations specifically addressing this issue. We recommended that SSA:

1. Initiate OMB-required breach-notification evaluation procedures upon notification that SSA mistakenly included living individuals' PII in the DMF.

2. 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.

In their response to our recommendations, Agency officials stated the number of death-reporting errors was small, and they expressed their concern with our characterization of these death-reporting errors as "PII breaches." Agency officials further stated that to the best of their knowledge, no case of fraud or abuse had occurred because of the DMF reporting errors. Nonetheless, SSA agreed to take a cautious approach and initiate breach-notification evaluation procedures in accordance with OMB guidance. SSA formed a task force that would assess Agency notification and remediation practices under OMB guidelines.

In late 2008, SSA hired a contractor (IDAnalytics) to perform risk analysis on about 27,000 individuals whose PII was erroneously included in the DMF. The contractor continues to perform this risk analysis on a continuing basis. According to SSA, as of November 2011, the contractor had not identified any victims of "organized misuse." As a result, SSA considers these cases "low risk situations" and has determined it was not necessary to provide notification

to any of the individuals whose PII was erroneously published in the DMF. SSA stated that if, in the future, the contractor identifies any individual who has been the victim of misuse, SSA will notify the individual and offer credit monitoring to them.

With regard to your question of whether SSA could implement a process similar to VA for notifying individuals when their PII is erroneously published in the DMF, yes, SSA could implement a similar process.

Thank you for the opportunity to address these issues. I trust that I have been responsive to your request. If you have further questions, please feel free to contact me, or your staff may contact Misha Kelly, Congressional and Intra-Governmental Liaison, at (202) 358-6319.

Sincerely,

Patrick P. O'Carroll, Jr.
Inspector General

MEMORANDUM

To: The Honorable Sam Johnson, Chairman
Kim Hildred, Staff Director
Subcommittee on Social Security, Committee on Ways & Means
U.S. House of Representatives

From: Patricia W. Potrzebowski, Ph.D., Executive Director
National Association for Public Health Statistics and Information Systems

Date: April 4, 2012

Subject: Responses to Questions from Hearing on Social Security Death Master File

---

Attached please find responses to questions for the record from the National Association for Public Health Statistics and Information Systems (NAPHSIS). NAPHSIS greatly appreciates the opportunity to contribute to this important dialogue.

If you have additional questions, please do not hesitate to contact our Washington representative, Emily Holubowich at eholubowich@dc-crd.com and 202.484.1100.

National Association for Public Health Statistics and Information Systems
Responses to Questions from Hearing on Social Security Death Master File

Subcommittee on Social Security, Committee on Ways & Means, U.S. House of Representatives

1. **You have indicated in your testimony that under our Constitution, States have the responsibility and the rights to manage vital statistics, which of course includes death records. If a system of accreditation is developed for sharing data amongs certified users, what should be the role of state death data and what considerations should be given to state sovereignty over this data? What suggestions would you have for making sure the states retain control of vital statistics both legally and in regards to personal privacy of their citizens?**

   Any system of accreditation that is developed for sharing state death record data among certified users would need to preserve the authority of each State for permitting access to the vital statistics data they provide to this system. That is, each state should have responsibility for and control over who accesses their own state provided death records. That consideration should be paramount, that is, it should override any other considerations.

   The easiest way to do this is to exclude all state provided death records, as is currently being done with the public DMF, but other alternatives are possible. The EVVE system allows each State to approve each data user. That means, for example, that State X, an open record state, can permit access to its death data by any certified requestor, but that State Y, which permits fact-of-death data to be provided only for government agency use, can limit access only to certified users that are government agencies. State Z, may permit access not only to governmen agencies, but also to organizations that can demonstrate a direct and tangible interest in the record (e.g. a credit card or life insurance company). This type of system would make sure that the states retain control of vital statistics both legally and in regards to personal privacy of their citizens.

   What level of reimbursement to the States should users pay?

   It is difficult to say exactly what level of reimbursement to the States users should pay for access to state death records, because different States set different fees. Many state vital records offices are funded solely through fees collected primarily from the sale of certified copies of birth and death records. In other states, the fees collected are used to offset state appropriated funds to support the vital records operation. This fee based revenue must cover all of the costs of collecting and processing the information that is contained in vital records, including the purchase and maintenance of computer systems; staff to operate data collection and quality control systems; staff to educate and work with the data providers (i.e., physicians, funeral directors, hospital and other health care facility staff, coroners, etc.) to ensure that vital records are complete, accurate, and submitted on a timely basis; staff to provide services to the public and other data requestors, including correction and amendment of records and issuance of certified copies, analyses and preparation of statistical reports and special requests for data; and other related costs.

   To protect state vital records offices from losing essential revenue, it is recommended that each user of state death data pay a fee to the state vital records office for each access to the death data. This fee would cover the loss of revenue that states incur and is consistent with the State position that they are providing a license to use the data for a specified purpose.

The current EVVE pricing model includes a monthly maintenance fee and a transaction fee for each query, as well as a fee when a match occurs. The match fees differ if the request is a verification (i.e., the user already has a birth or death certificate for the person being queried) or a certification (i.e., the person querying does not have a birth or death certificate for the person being queried). Match fees are set by the individual states. NAPHSIS would be happy to work with the States to evaluate and consider revisions to the current EVVE pricing model based on new uses of EVVE.

2. **I assume that your group, that represents all the vital statistic bureaus throughtout the US., is not a part of this interagency working group. Yet, you have clearly shown us that under our system of federalism, states have the responsibility for managing their vital statistics records. What should this group keep in mind as they consider options and what recommendations would you have for this interagency group?**

NAPHSIS is not part of the interagency working group. NAPHSIS would be pleased to participate on or meet with the working group to provide information and to answer questions. NAPHSIS recommends that the interagency working group keep the following key points in mind as they consider options and recommendations for use of state death data:

(1) Assure that State Provided Death Records are Not Released to the Public

The interagency working group should understand that access to identifiable death records differs based on state statutes. In a few states this information is public information, while in most states access to identifiable death record data is limited to family members or others with a direct and tangible interest, government agencies, or for medical research purposes. Some states prohibit commercial use of vital records data. It should be noted that this is different from the Federal Privacy Act, under which a person who is deceased is no longer afforded the right to privacy. Because state statutes differ, it is critical that state death records continue to be excluded from public release by SSA or any other government agency, without the prior approval of the appropriate state vital records office.

(2) Prevent State Loss of Essential Operating Revenue

Many state vital records offices are funded solely through fees collected primarily from the sale of certified copies of birth and death records. In other states, the fees collected are used to offset state appropriated funds to support the vital records operation. This fee based revenue must cover all of the costs of collecting and processing the information that is contained in vital records, including the purchase and maintenance of computer systems; staff to operate data collection and quality control systems; staff to educate and work with the data providers (i.e., physicians, funeral directors, hospital and other health care facility staff, coroners, etc.) to ensure that vital records are complete, accurate, and submitted on a timely basis; staff to provide services to the public and other data requestors, including correction and amendment of records and issuance of certified copies, analyses and preparation of statistical reports and special requests for data; and other related costs.

To protect state vital records offices from losing essential revenue, it is recommended that the interagency workgroup require that each proposed new government user of state death data pay a surcharge to the state vital records office for each new use. This surcharge would not increase SSA's costs, but would be passed through to the other government agency users of the state data. This

surcharge for the state vital records offices would cover the loss of revenue that states would incur by the expanded use of state death data for government agency use. This is consistent with the State position that they are providing a license to use the data for a specified purpose.

(3) Prohibit Re-Release of State Data

Again, consistent with the States providing a license to use their data for a specific purpose, the state vital records offices recommend that any provision of vital records data to a government agency after payment of the negotiated surcharge (license fee) must not be permitted to be re-released for the same use to any other organization/entity, either public or private (e.g., local or state government partners or any other grantees) without prior state vital records office approval. Nor can a government agency use the state death data provided for an additional use not specified in the initial request. Prohibiting such re-release will protect state vital records offices from the loss of essential revenue and help assure that the data are used only for allowable and approved purposes under state law.

(4) Limit Use to Administrative, Non-Research Purposes

The National Death Index (NDI) was established in 1979 by the National Center for Health Statistics (NCHS) in the Centers for Disease Control and Prevention (CDC) for use by medical or health researchers to determine if study subjects have died anywhere within the United States without the researcher having to contact each state vital records office. State vital records offices provide their death record information to the NDI, including cause of death information (NDI Plus). When researchers use the NDI Plus, they pay a surcharge to NCHS that is then shared with state vital records offices. The state vital records offices are concerned about loss of existing revenue if their death data is permitted to be used for research purposes. They therefore recommend that no state death data be permitted to be used for research uses and that government agency use be limited to administrative uses only.

(5) Delay Public Release to Allow Time for Birth/Death Matching by States

The Intelligence Reform and Terrorism Prevention Act of 2004 requires state vital records offices to match birth and death records once a death has occurred, and to mark the birth record "deceased." This is critical for protecting against identity theft, but it cannot happen instantaneously, particularly when a person dies in a different state than s/he was born. It takes some time for the death record to be transmitted to the state of birth and for the birth record to be marked as deceased. Not all states are currently participating in the electronic State and Territorial Exchange of Vital Events (STEVE) system, so in nearly half the states, this is still a manual process. In order to protect publicly provided death records from being used for identity theft, the state vital records offices recommend that a time lag of 60 days after the date of death be considered for any public release of death records. This time will allow state vital records offices to match the death record with the decedent's birth record and to mark the birth record "deceased," thus preventing the birth record's use for identity theft.

3. **With 57 different vital record jurisdictions managing death data, I am sure there are many variations. Can you describe for us in general the policy States use to govern data?**

Access to identifiable death records differs based on state statutes. In a few states, this information is public information, while in most states access to identifiable death record data is limited to family members or others with a direct and tangible interest, government agencies, or for medical research purposes. Some states prohibit all commercial use of vital records data.

In most states there is a charge for providing death information (similar to a license to use the information) and generally—with the exception of a family member or their legal representative who must submit an application for a certified copy of the death record—a requestor must also sign a data use agreement. The data use agreement specifies the data provided, the purpose for which the data are requested, prohibits re-release, and requires the requestor to agree to a number of conditions to protect the confidentiality and security of the information provided.

4. **Do States allow access to their data? If so, to whom and for what purposes and are certain data elements redacted or restricted?**

A few states allow public access to their vital statistics death data. In some states the access is restricted at the state level but is concidered to be public information at the local government level (e.g., town clerk or local registrar).

All states permit family members or next of kin to apply for and purchase a certified copy of the death record. Most states permit government agencies to obtain selected data elements, but only those needed for the specific government agency use. Many states permit medical or health researchers to obtain selected data elements, but only those data needed for the research. For medical/health research or for government agency use, many states restrict access only to certain needed data elements. In some states, the cause and manner of death are restricted or redacted for almost all purposes, unless specifically authorized.

5. **Do some States sell data to other government or private buyers?**

Yes, some states "sell" data to government agencies, but this is more accurately characterized as a "license" for the government agency to use the data for a specific purpose. Some open record states may sell data to private buyers, generally on a record by record basis, although it is possible that a few states sell entire data files.

6. **You spoke about a system, similar to a computer hub-like system, that takes electronic queries from government agencies to confirm birth and death information from the records of the other states. You called this the Electronic Verification of Vital Events. Tell us exactly how this works, if it might open some day to commerical users and if this system might be the solution for certain types of data authentication problems.**

Many Federal and State agencies rely on birth certificates for proof of age, proof of citizenship, identification for employment purposes, to issue benefits or other documents (e.g. driver's licenses, Social Security cards, and passports) and to assist in determining eligibility for public programs or benefits. NAPHSIS has developed and implemented the Electronic Verification of Vital Events (EVVE) system, which provides the capability to quickly, reliably, and securely validate birth and death information. Via a single interface, authorized Federal and State agency users can generate an electronic query to any participating vital records jurisdiction throughout the country to verify the contents of a paper birth certificate or to request an electronic certification (in lieu of the paper

birth certificate), irrespective of the place or date of issuance. An electronic response from the participating vital records jurisdiction either verifies or denies the match with official state or jurisdiction records.

EVVE also provides an indication to the requestor if the birth record matched via EVVE has been marked deceased. The EVVE system is also capable of supporting the electronic verification and/or electronic certification of death records. The EVVE system supports real-time queries as well as batch queries. If the state of birth or death is not known, a broadcast system is available for electronic certification requests.

The EVVE system works by accepting a query from an approved agency user. That query is sent to the EVVE hub, which will then forward the query to the vital records office where the birth or death occurred. There is a piece of EVVE that is installed in each vital record jurisdiction infrastructure that accepts the query and checks the data entered as part of the query against its birth or death database. The results of the query are sent back to the EVVE hub, and then forwarded onto the originating requestor. Queries and their responses are sent over the internet, in an encrypted standard XML messaging schema, so confidential data is secure and protected. The EVVE system has also been certified and accredited by an independent organization to be compliant with the NIST 800-53 moderate level security standards.

The following Federal and State agencies have used the EVVE system: Department of Motor Vehicle Agencies, Medicaid Offices, Social Security Administration, Office of Personnel Management, District Health Offices, Army National Guard, and Department of State Fraud Prevention Offices.

While the EVVE system is currently limited to government agencies, it is possible that it may in future become available for commercial users, and would then be the solution for certain types of data authentication. The reason this approach would work is that with the EVVE system, each vital records office has the capability to approve or disapprove each requested user of EVVE for their own state's data.

NAPHSIS is currently developing possible solutions that would establish alternatives to assist authorized public and private sector entities to access state fact-of-death data for legitimate needs where state laws permit.

7. **The future of good statistic management seems to lie in more use of electronic death record systems. As more States send electronic death records (EDRs) to Social Security, there should be fewer erroneous reports of living persons put on their death roles, correct?**

Each State/jurisdiction submits to SSA death data for each death record filed in their State/jurisdiction. The development of an EDR system will improve the timeliness of receiving death data, along with its completeness and accuracy, especially if the EDR system has incorporated the process of verifying the decedent's SSN. If the EDR system incorporates a verification check of the SSN, the results of that verification are submitted to SSA with the death record.

Generally state death records are very accurate and complete, and only rarely do errors occur. However, if SSA continues to use sources other than EDRs from state health departments for reporting of deaths, and if the EDRs from those states do not override reports from other sources,

erroneous reports of the deaths of living persons could still exist in SSA death files.

8. **You mentioned that Social Security once helped underwrite funding for electronic death registration systems in the various States, but that funding has ended. You also stated that $20 million could insure these electronic systems in all States and jurisdictions. That capability would not only be good for Social Security but the other nine federal agenices that share Social Security's database for benefit management. Describe in more detail what the funding would support.**

   Additional funding would be used to support the development and implementation of electronic death registration (EDR) systems in those States/jurisdictions that do not currently have an EDR system. The additional funding would also be used to support the rollout of the EDR system to the death data providers, in those states/jurisdictions that need to develop their EDR system, and those states/jurisdictions that have already developed their EDR system but need to bring additional death data providers on-line so that the death records can be completed and filed electronically. With an EDR system, there are many death data providers that need access to the EDR system and training on how to use the EDR system. In most states and jurisdictions, this includes funeral directors, funeral home clerks, medical examiner and coroner offices, hospitals, physicians, nursing homes, and other entities that may certify the cause of death. Also, state and local registrars need to be on-line with the EDR system. So this funding will be used for development, implementation, and rollout of EDR systems in the states/jurisdictions.

   Would the development of EDRs eventually bring down the cost of accessing death data while increasing its security and if so, explain further these posiitive factors?

   The development of an EDR system will improve the timeliness of receiving death data, along with its completeness and accuracy. Edit checks on the data are incorporated into an EDR system to ensure that data quality is maintained. For example, an EDRS will prompt the user if the user indicates that a two year old decedent has a college education so they can review the data they have entered. An EDR system can also be integrated with the on-line verification of SSN (OVS) system to perform a real-time verification of the decedent's SSN.

   An EDR system will increase the security of death data, along with timeliness and quality, but NAPHSIS does not envision an EDR system bringing down the costs of accessing death data. EDR systems are costly to develop, implement, rollout, and maintain. There are additional IT costs associated with an EDR system that you would not have in the 'paper' manual registration environment. In other words, the costs are not decreased, but are shifted.

9. **If a third party such as your organization is able to provide the information to entities using vital statistics for legitimate and lawful reasons, is there a way to have data that is searchable and compatible with the entities that need this information?**

   We are not aware of any serious technical barriers to having data that are searchable and compatible with the entities that need identifiable fact-of-death death information for legitimate and lawful reasons. Rather the critical issue is related to the differing State statutes and regulations that govern access. That is why the EVVE system, which allows each State to decide on a case by case basis which users would be permitted to access their State's death data is a feasible alternative for some users.

[Submissions for the Record follow:]

Afro-American Genealogical & Historical Society of Chicago, Inc.

January 30, 2012

Judith Samuel, President
Afro-American Genealogical & Historical Society of Chicago
P.O. Box 377651, Chicago, IL 60637-7651
Telephone: 773-602-2743
Email: aaghsc@yahoo.com

Re: **Chairman Johnson Hearing on Social Security Death Records, February 2, 2012.**

To: The House Committee on Ways and Means, Subcommittee on Social Security

U.S. Congressman Sam Johnson (R-TX), Chairman of the House Committee on Ways and Means, Subcommittee on Social Security will hold a hearing on the accuracy and uses of the Social Security Administration's Death Master File. I am submitting the following information to be submitted into the hearing record.

The Afro-American Genealogy & Historical Society of Chicago stands with the Records Preservation and Access Committee (RPAC), an umbrella organization representing the genealogical community, in maintaining access to the Social Security Death Index (Death Master File).

Genealogists rely on Social Security numbers to correctly identify individuals.
We share Congress' concern about protecting Americans from identity theft. In that regard, RPAC notes that rarely has it been documented that an individual's identity is violated by access to the SSDI; rather, the violations occur due to computer breaches from government and private enterprises.

Please consider the legislative suggestions submitted by RPAC to address deficiencies in the current operation of the Death Master File.

We ask that you protect genealogists' access to the Death Master File which is vital to documenting our family histories.

Sincerely,

Judith Samuel, President
Afro-American Genealogical & Historical Society of Chicago

cc: Board of Directors

Comment on Hearing on Social Security's Death Records

Name:	**Mary Ann Boyle, PhD, CG**
Organization:	**American Genealogical Research and World Data**
Address:	**8 Whittier Place, Suite 23G, Boston, MA 02114**
Phone number:	**617-742-6063**
Email:	maryann@agrboston.com
Title of Hearing:	**Social Security's Death Records**

I am writing to state the importance of the identifying information included within the Social Security Administration Death Index (SSDI). I use the SSDI every day in my forensic genealogical practice.

To gain an appreciation of the value of the SSDI for the accomplishment of my work, I would like to offer a brief explanation of my business. I have worked full time for 22 years exclusively conducting forensic genealogical investigations for attorneys and trust officers. While I work on a variety of types of legal cases; all involve identifying, locating and documenting people for the purpose of distribution of assets.

My expert testimony, written and/or oral, is required for the purpose of identifying individuals defined by appropriate statutes. In the case of an administration of an estate, the individual state statues define in genealogical terms the heirs-at-law who are eligible for inheritance. By collecting documentation about the family members and analysis of the data, we are able to offer the court-quality evidence to support the heirs. Each person in the family must be identified using as many primary documents as possible. The SSDI is critical to the performance of this research. Often we are working with no clues from the family about the fate of other family members many of whom may be deceased. In each case the available identifying data for individuals varies but commonly we have almost nothing. Each of the components of the SSDI are useful in identifying family members.

Other types of cases on which we are asked to provide expert testimony are probate of wills, clearing titles to real estate, guardianships, ownership of intellectual property, and distribution of assets from trusts.

Feb. 13, 2012

TO: House Ways and Means Committee

FROM: Alex E. Friedlander
53 Tidy Island Boulevard
Bradenton, Florida 34210
941-792-9618
aefgen@aol.com

STATEMENT CONCERNING HEARING ON SOCIAL SECURITY'S DEATH RECORDS

The purpose of this statement is to register my strong opposition to the possible discontinuation of public access to the Social Security Death Index, which I understand is being considered by your committee as a means to reduce fraudulent use of deceased person's names in filing false income tax returns.

The Social Security Death Index is accessed by many different companies, non-profits and other entities besides individuals like myself who are researching their family history. Forensic specialists utilize the SSDI when reuniting remains of military veterans with their next-of-kin and descendants. Law offices, banks and insurance companies utilize the SSDI to resolve probate cases and to locate heirs. Organizations that help child survivors who were orphaned by the Holocaust to find family use the Social Security Death Index in locating relatives. The loss of this resource will be a major setback for the work of all these varied parties.

To penalize all the legitimate users of the SSDI in order to prevent the fraudulent use of the SSDI by a few persons is not the best way to solve the problem. One solution being proposed is to have the government itself use the SSDI to match against filings to check for false claims. Another would be to redact the Social Security numbers from this index. A different although less helpful solution for those who use this index legitimately would be to delay the addition of names to the index for a specified time period after the death of the individual.

I hope you will seriously consider my comments, and those of many others who are concerned with the possible loss of this valuable resource, and find better ways to solve the problem you have identified without restricting access to this important index.

Dr. Alex E. Friedlander

I am seriously concerned with the potential negative impacts of H.R. 3475 introduced by Sam Johnson (R-Texas). Because of tax fraud and other abuses of the publicly available Death Master File (DMF) and the associated Social Security Death Index (SSDI), the bill, according to Rep Johnson's press release, would "would stop Social Security from making this information public."

This would harm legitimate research such as for:

Family medical history in tracing inherited conditions,
Associating DNA of dead soldiers with the correct family,
Helping coroners find next of kin,
Use as a tool by credit reporting agencies, merchants, and private investigators,
A data asset available to over nine million genealogy hobbyists.

There are many legitimate public research uses of the DMF and the SSDI. The data aids in resolving probate issues, in finding relatives, and in working genealogy. Congress should investigate methods of improving the documentation of reported deaths. The Internal Revenue Service should verify that Social Security Numbers belong to individuals old enough to legally work and that SSNs do not belong to individuals previously reported as youthful family members in previous years. Institutions in the commercial sector must make better use of the data available to them.

I am doing my family tree and i would like you to know how important this is to me that you do not block access to the social security number dead file. i rely on these numbers quite a bit to locate family members who have passed away. i am not alone. many of your constituents are genealogists and we all would like you to reconsider your bill. we are totally against it and it will greatly stunt our continuing research.
please look for another alternative to your plans. there are other ways to stop i.d. fraud, and all of the other reasons you gave for moving forward with your
proposal.
thank you, andrea dudley, 38456 16th st. wyandotte mi. 48192
734-250-1678

February 3, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Anita Scarborough
105 Sturbridge Lane
Chapel Hill, NC 27516

Dear Committee members - I am not sure that I understand the reasoning behind the debate to close off the Social Security Death Index. This a valuable source of information for those of us who are pursuing our past. Social Security records have enable many of us to trace our ancestry and locate living relatives. It would seem that this information should be available to us by way of the provisions of the Freedom of Information Act which was enacted many years ago to make our government more transparent. You might also be cutting off an important source of revenue since accessing these genealogical records requires a fee to possess. I am co-president of the Italian Genealogical Group. We host a tremendous data base of vital records for our ancestors on our web site. These records have enabled our membership to make the journey back to their ancestral roots. Sealing the SSDI would rob us of these essential ancestral records and make our journey back to the future that much more difficult. I urge you and the members of your committee to recommend that the SSDI continue to be available to us.

Yours turly,

Anthony Di Bartolo,

Co-president of the Italian Genealogy Group

V.P of Public Relations

www.italiangen.org

516-672-8980

tonyhp13@gmail.com

16 February 2012

STATEMENT FOR THE RECORD, HOUSE COMMITTEE ON WAYS AND MEANS, SUBCOMMITTEE ON SOCIAL SECURITY, WRITTEN COMMENTS ON PROVISIONS RELATING TO SOCIAL SECURITY ADMINISTRATION'S DEATH MASTER FILE, ALSO KNOWN COMMERCIALLY AS THE SOCIAL SECURITY DEATH INDEX.

I. INTRODUCTION:

The House Committee on Ways and Means, Subcommittee on Social Security, held a hearing on 2 February 2012, regarding the accuracy and uses of the Social Security Administration's Death Master File. The genealogical community was informed that no invitation to testify at the hearing would be forthcoming, but we were invited to submit a statement. This statement is accordingly submitted on behalf of the **Association of Professional Genealogists (APG).**

II. APG BACKGROUND & CONTACT INFORMATION:

The **Association of Professional Genealogists** (http://www.apgen.org), established in 1979, represents more than 2,400 genealogists, librarians, writers, editors, historians, instructors, booksellers, publishers and others involved in genealogy-related businesses. APG encourages genealogical excellence, ethical practice, mentoring and education. The organization also supports the preservation and accessibility of records useful to the fields of genealogy and history. Its members represent all fifty states, Canada, and thirty other countries.

The mission of the Association of Professional Genealogists is to support those engaged in the business of genealogy through advocacy, collaboration, education, and the promotion of high ethical standards.

Association of Professional Genealogists
PO Box 350998, Westminster, CO 80035-0998
tel. 303-465-6980 fax 303-456-8825
e-mail: admin@apgen.org – Kenyatta D. Berry, APG President

Contact for purposes of this statement:
Debbie Parker Wayne, Certified Genealogist and APG Region 2 Director
PO Box 397, Cushing, TX 75760-0397
tel. 936-326-9101
e-mail: debbieparkerwayne@gmail.com

III. APG STATEMENT:

Thank you for the opportunity to present our concerns regarding the proposed elimination or reduction of public access to the commercial version of the Death Master File (DMF), the Social Security Death Index (SSDI). For the purposes of this statement, we will be addressing access to the SSDI rather than the DMF, as the SSDI is the version that genealogists are permitted to access.

We were disappointed and concerned that the genealogical community was not invited to participate at the February 2nd hearing. The Records Preservation and Access Committee (RPAC) is a consortium of organizations of the genealogical community, an important stakeholder in the proposed legislation. RPAC has been working tirelessly with the Subcommittee staff since mid-November – providing information on genealogists' use of the SSDI and suggesting legislative language to deter identity theft while retaining public access. **The Association of Professional Genealogists is even more concerned as many of our members earn all or part of their income from genealogical research. Access to the SSDI is critical to the success of many of our cases.**

It is ironic that a system that should be used to prevent identity theft (by permitting employers, financial organizations, insurance companies, pension funds, and others the ability to check names against those deceased as reported on the Death Master File),[1] is now being determined—inappropriately and with no evidence supporting the conclusion—as an instrument of identity theft. We support the Subcommittee's intent to protect the residents of the United States from improper usage of their personal information, and to protect them from identity theft. But rarely has it been documented that an individual's identity is violated by access to vital records or the SSDI; rather, the violations occur due to computer breaches from government and private enterprises and thefts from individual homes. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen."[2] Many of these computer breaches have been well documented in the press.[3] The Federal Trade Commission reports identity theft is more commonly the result of theft from discarded mail, theft of purses and wallets, and con jobs where thieves obtain confidential information through deceptive schemes.[4]

Removal of the SSDI from public access would not necessarily reduce the problem of fraudulent use of a Social Security number. As it will no longer be available as a reference check to many who use it as an identity theft deterrent, it may well increase identity theft. If government agencies and business firms used the SSDI to confirm Social Security numbers of deceased persons are not being used improperly or illegally the SSDI could reduce the problem.

---

[1] http://www.ntis.gov/products/ssa-dmf.aspx

[2] http://www.identitytheft.info/breaches09.aspx

[3] http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer breach/ http://www.nctimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html http://www.qctimes.com/news/local/article_06d38e24-146a-11df-91c6- 001cc4c03286.html http://www.washingtonpost.com/politics/tricare-military-beneficiaries-being-informed-of-stolenpersonal-data/2011/11/23/gIQAcRNHtN_story.html http://sundayherald.com/news/heraldnews/display.var.2432225.0.0.php Copes, H., and Vieraitis, L.M. (2009). Understanding identity theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, *34*(3), 329-349.

[4] http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/about-identity-theft.html

Professional Genealogists

Professional genealogists depend on the access to the SSDI for our livelihood. In addition to performing research for clients interested in their personal family history, professional genealogists work on many cases that cannot be solved without the information available in the SSDI. Some of those cases include:

- Identification and location of potential DNA donors to allow confirmation of identity for deceased American military servicemen and women. This POW/MIA personnel repatriation project generates enormous positive press for the U.S. government.[5]

- Identification and location of next of kin for unclaimed deceased persons. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope.[6] When the families can be found, this saves the government the expense of burial.

- Identification of next of kin to notify families prior to cemetery relocations.

- Identification of heirs in probate and estate settlement cases for the courts and for trust and insurance accounts.

- Identification of rightful owners in oil, gas, and mineral royalty cases.

- Many other important property and civil rights issues that require identification of living individuals in order for them to receive benefits due them.

The majority of professional genealogists work as small, single-person businesses. Subscriptions to databases such as LexisNexis, used by attorneys, are beyond the means of these small businesses. The loss of the SSDI could easily:

- force many professional genealogists out of business further adding to the economic woes facing our country today, and

- increase the costs to the U.S. military, courts, and other governmental agencies with mandates to locate family members to settle cases and for repatriation purposes.

IRS Needs to Be More Proactive

If the IRS were to routinely run Social Security numbers included in tax returns against the death index, they might avoid giving refunds to deceased individuals. "Operation Rainmaker" (also known as Operation TurboTax), was a tax fraud operation in the Tampa Bay area. Law enforcement interviews specified that the IRS, while cooperating with other law enforcement officers, is not

[5] http://articles.cnn.com/2010-12-09/us/wwi.soldier.remains_1_mia-accounting-command-missing-personnel-office-larry-greer?_s=PM:US
[6] http://unclaimedpersons.org

authorized to share information with local law enforcement departments, hampering efforts to protect their citizens. If the federal government is serious about addressing identity theft that uses a person's Social Security number, then the IRS needs to be given legislative authority to share information with local, county and state law enforcement organizations. It was also stated that filing tax refunds for under $10,000 will not get any attention. As "Operation Rainmaker" found the average tax fraud was about $9,500, below the $10,000 threshold.[7] This is another practice that the Congress needs to review, as the criminals who are perpetrating this fraud know they will be undetected.

It also became apparent in Mr. Agin's testimony to the Subcommittee hearing on 2 February 2012 that the IRS assumes the first person filing is the "legitimate" filer and by inference, the second filer is the fraudulent party. The IRS needs to amend their practice when the filing involves a deceased child, to require some verification to determine which is a valid filing. Unfortunately, since the IRS advocated electronic filing of tax returns, one unexpected consequence is the remarkable increase in tax identity theft.

Support For Efforts to Cease Identity Theft

Genealogists are strongly opposed to identity theft and support efforts to stop it immediately, using tools already available to government agencies. For example:

- If income tax returns were electronically compared to the Master Death File, matching cases could be flagged for special processing, and the person attempting to create a tax fraud could be stopped before the fraud occurs.

- A parent's social security number should be required when filing a tax return for any minor. It is an extremely rare occurrence that a minor child would not be listed as a dependent on the parent or guardian's tax filing. If the minor dies, the IRS could have a procedure to flag any filings without the parent's social security number, again preventing the fraud. Draft legislative language was provided to the Subcommittee staff on January 24, which would facilitate just this prevention of identity theft perpetrated on children.

- The *National Taxpayer Advocate's Report to Congress for 2011* specifically highlights the benefits of the IRS Issued Identity Protection PINs[8] and suggests that taxpayers should be allowed to turn off their ability to file tax returns electronically. Any family that suffers a death could elect to turn off the electronic filing ability.

- Criminal penalty statutes for those who fraudulently use Social Security Numbers, including, but not restricted to, those who misuse their positions (*e.g.*, hospital, medical institution and office personnel, financial and credit card organizations personnel, prison corrections officer, college or university registrar etc.)

---

[7] http://www.youtube.com/watch?v=gpgTFO7nMBk
[8] http://www.irs.gov/pub/irs-pdf/p2104.pdf

For the reasons stated above:

- genealogists are **NOT** the cause of identity theft;
- genealogists have legitimate, professional and lifesaving reasons to have immediate access to the SSDI; and
- proactive measures are needed to prevent identity theft and vigorously pursue and punish the **TRUE** identity thieves.

APG respectfully and vehemently encourages the Subcommittee to continue the commercial version of the Death Master File, known as the Social Security Death Index, to be available to the public.

On behalf of the Association of Professional Genealogists we appreciate the opportunity to submit our comments, and for the occasion to bring to the Subcommittee's attention the many services the professional genealogical community performs for local, **state and federal government offices.** We look forward to working with the Subcommittee and staff to find an accommodation that provides genealogists with continued immediate access to the SSDI.

Respectfully submitted,

Kenyatta D. Berry
APG President

Debbie Parker Wayne, Certified Genealogist
APG Region 2 Director

APPFA
PO Box 16064
Columbus, OH 43216-6064

House Committee on Ways and Means Office
Subcommittee on Social Security
1102 Longworth House Office Building
Washington, DC 20515

Dear Committee Members,

You are receiving this letter today because we, the members of the Association of Public Pension Fund Auditors (APPFA) are seeking your assistance to protect the finances of public pension funds throughout the United States. Since you may not be familiar with our group, we will provide some background information. APPFA's membership is comprised of the internal auditors of over 85 state and local public pension systems throughout the United States. The organization provides semi-annual conferences to provide members with continuing education and a forum for networking and sharing concerns about the risks facing each of our respective systems and/or the public pension system industry.

While as a group we help oversee more than a trillion dollars in assets, the common misconception is that the predominant risk concerns the protection of our investments. However, our systems' investments are well diversified and appropriately controlled. Public pension systems face an enormous amount of risk in protecting the outflows of funds. We must ensure that benefit payments are accurately calculated, are only made to eligible recipients, and are terminated upon the death of the recipient. It is the last point that prompts us to write this letter seeking your assistance.

Advancements and access to electronic public death records in the U.S. over the past 30 years has allowed each of our pension systems to greatly improve controls to guard against overpayment of benefits resulting from the death of our members. Often times these overpayments are being fraudulently converted for personal use by those individuals close to the deceased beneficiary. Many different approaches are employed by the nation's pension systems. Most pension funds use one or more of the following approaches to obtain death information of their members:

- Direct interface with state or local vital statistics agencies.
- On-line access to public records through services such as LexisNexis or Accurint.
- Contracting with business partners such as Pension Benefits Information (PBI), the Berwyn Group, or others that accumulate national death records and match the funds membership data against their death files to identify matches (potential member deaths).

Access to this data through these agencies and services has saved APPFA's member systems millions of dollars in potential losses due to overpayments and fraud.

APPFA is very concerned about recent restrictions on the data that the National Technical Information Service (NTIS) provides in the Social Security Administration (SSA) Death Master File (DMF), the primary source of death data. A recent interpretation by the Social Security Administration of the legislation contained in Section 205 (r) of the Social Security Act has created a gap in the death information that is provided to our pension systems. Our members no longer have access to death data that is provided under contract to the SSA from various states. As a result of this change, the amount of death information has declined by approximately 50%. This has undoubtedly led to overpayments to deceased annuitants and beneficiaries at a time when the public pension industry can least afford to erroneously pay out millions of dollars.

Prior to November 1, 2011, our organizations had access to the complete Death Master File which helped to ensure that we were only paying monthly benefits to live annuitants and beneficiaries. On behalf of the members of the Association of Public Pension Fund Auditors throughout the United States, we urge you to pass legislation to allow authorized government users such as public pension funds and authorized death verification vendors' unrestricted access to the complete Death Master File. Authorized government and death verification vendors will have no hesitation to agreeing to any confidentiality clauses in any contract with the Social Security Administration because these users do not publish anyone's Social Security Number living or deceased and take these confidentiality clauses very seriously. Should you have any further questions about this letter, please contact me.

Thank you for considering our request.

Sincerely,

Steve Hayward

APPFA President

Website: www.APPFA.org

Email: shayward@surs.org

U.S House of Representatives

Washington, DC

Arthur Whelan
285 Borel Circle
Palm Bay, FLA
32907

RE: SSDI = Social Security Death Index -- Keep it Public

Dear Congressional Rep.: FEB, 2012

This is to urge you ***Not*** to pass HR 3475, which would close public access to the SSDI, which is a resource of great value in several areas. I believe you have reports from RPAC - the Records Preservation & Access Committee. This details the public use of the SSDI, which is a **Pro-Security** asset in preventing identity theft. Someone using the SS **#** of a dead person - unless working on probate - may be up to no good. Businesses and law enforcement agencies can readily use the SSDI in checking on such cases.

I am an amateur genealogist - or family historian - with 15 years of experience, and a member of the Genealogical Society of South Brevard since 2000. This society, with a website at gssb.net , is located in Melbourne, FLA.

Accredited professional genealogists use the SSDI for important purposes. These include assisting coroners in finding kin of deceased persons, and helping families with medical history and DNA investigations - **which can Help Save Lives.** They also help families of missing/deceased military members. Please contact RPAC for more info. if needed - though I hope you already have that.

My own use of the SSDI over the years illustrates another important use:
The SSDI fosters Family Values at their best.

Using the "final locations" on the SSDI, I have been able to order many obituaries, which usually list survivors, whom I can then contact with a friendly letter and one or more pictures of common kin. Those survivors are free to respond, or not -- most do respond and are glad to hear from me. This has led to ongoing correspondence, sharing of photos and other information, and even in-person visits and gatherings. Following are three notable examples of that.

Via the SSDI, we contacted a CT family. They visited NY, where we were able to take 3 cousins to the Brooklyn home where their father lived as a young man--a very moving experience for them. This family had been looking for us. They were delighted to hear from us, and we have been in touch ever since with these wonderful people.

This family had 6 branches. Because of SSDI access, I was able to contact surviving members of the other 5 branches and send them prints of this grand classic portrait. **All** were most grateful.

The lady at front right is a living 1st cousin of my father Adrian Whelan (1912-1957), contacted via the SSDI. We have met in person and exchanged many pictures and stories for several years now.

These are outstanding examples of the value of the **Public SSDI** for family history and Family Values. For this - and the other positive uses of the SSDI - I urge you to keep this index public.

Sincerely, Arthur Whelan

Respected Leaders, I am writing today to voice my dismay and disapproval in regards to this bill. Restricting public access to such information will cause much disappointment. In keeping these records closed up as information not to be accessed by the public many of us will know our family lineage This may not seem to bother you on the surface but, the stress one feels when they seek answers abooout their ancestors is very real. Please do not cut out one more place in which to search for the outside. Have a great week.

Bette Mae Ritchotte

80 South Main St Shickshinny, OA 18653

bettemae@pa.metrocast.net

I pray you keep the thousands of us who wade through so much information in search of one more piece, Don't freeze yourself tonight in the cold....be careful in deciding.

Feb. 02,2012

Blanche M. Wallace
1420 W Harvard St
Orlando, Florida 32804
407-423-0094
blanchew@bellsouth.net

February 4, 2012

Re: Social Security Death Records Hearing - "Keep IDs Safe Act"

This is written on my own behalf as a family historian who uses the Social Security Death Index (SSDI) to research the history (especially, the medical history) of my family. Using the SSDI to obtain the place and date of death allows me to request the correct death certificate from the appropriate state agency. The medical histories created from this research allow the living to better inform and plan ahead with their physicians. Without access to the SSDI, this type research would be eliminated or severely hampered.

Obituaries (print and digital) provide date of death and can easily be used by criminals for the purpose of identify theft. However, obituaries rarely mention the cause of death so they can't be used for the purpose of tracking ancestral medical history.

In fact, the SSDI is a deterrent to identity theft according to the National Technical Information Service (NTIS) website (http://tinyurl.com/yb6e49e) which states that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. In addition to family history researchers, the SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Rarely has it been documented that an individual's identity is violated by access to the SSDI; rather, the violations occur due to computer breaches from government and private enterprises. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen"[1]. Many of these computer breaches have been well documented in the press.[2]

1. http://www.identitytheft.info/breaches09.aspx
2. http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer_breach/
http://www.nctimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html
http://www.qctimes.com/news/local/article_06d38e24-146a-11df-91c6-001cc4c03286.html

Your consideration of these points in favor of maintaining open access to the SSDI will be appreciated.

Thank you.

Leslie Brinkley Lawson,
President
Council for the Advancement of Forensic Genealogy
5180 SW 198th Av
Aloha OR 97007-2964
503-649-6679
Leslie@LawsonResearch.net

Dee Dee King, Certified Genealogist,
Secretary-Treasurer
Council for the Advancement of Forensic Genealogy
PO Box 1085
Manvel TX 77578
281-431-3525
King@forensicgenealogyservices.com

Chairman Johnson Announces a Hearing on Social Security's Death Records
Submission for the record: waysandmeans.submissions@mail.house.gov

The Council for the Advancement of Forensic Genealogists supports open public access to the SSDI, Social Security Death Index, the commercial term for the Social Security Administration (SSA) Death Master File (DMF).

As professionals trained to cite the sources of facts used in our reports, we find it alarming that testimony presented during the House Ways and Means Sub-committee on Social Security's Death Records failed to cite a single source which proved that access to the DMF/SSDI was used to perpetrate fraud. Indeed, a minority of such cases may exist; however recent studies fail to mention DMF/SSDI as a proven source for fraud.[1]

The heart-wrenching testimony of Mr. Jonathan Agin concluded with his open admission that he could not prove that the DMF/SSDI was the source for the fraud perpetrated upon the Social Security number of his deceased daughter. Mr. Agin clearly admitted that it was only his *assumption* that DMF/SSDI was the source and that other possibilities existed.

Social Security Commissioner Michael J. Astrue testified that the original purpose of the DMF/SSDI was to prevent fraud through its open access by banks and other financial institutions. Commissioner Astrue went on to state that the use of the DMF/SSDI has changed over the years, and that some of that change has included use for fraudulent purposes. However, the Commissioner failed to cite a single source of evidence that proved DMF/SSDI was the

[1] Federal Trade Commission (http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html : accessed 15 February 2012).Privacy Rights Clearing house (http://www.privacyrights.org/ar/idtheftsurveys.htm : accessed 15 February 2012).National Institute of Justice (http://nij.gov/topics/crime/id-theft/welcome.htm : accessed 15 February 2012).Javelin Strategy & Research (https://www.javelinstrategy.com/brochure/192 : accessed 15 February 2012).

source for fraud.

DMF/SSDI has evolved into a tool used to prevent fraud by many more entities than those originally intended, the banking and financial institutes. Human resource departments large and small depend upon access to the DMF/SSDI in order to meet federal guidelines on hiring. These federal hiring requirements not only address fraud, but also aspects of our nation's war against terrorism.

DMF/SSDI has also become an invaluable resource to those who conduct **genealogical** research, both privately and in the public and business sector. Testimony during the Sub-committee's hearings appeared to make scapegoats of the genealogists and the use of DMF/SSDI for **genealogical** purposes.

Genealogical research is a matter of using various tools to accumulate data to discover the truth. DMF/SSDI is an irreplaceable resource used across the commercial spectrum, such as attorneys, bank and trust companies, title companies, oil and gas companies, medical researchers, forensic genealogists, and others.

A few examples of **genealogical** usage are:

- The Department of Defense is mandated by Congress to repatriate the remains of our unaccounted-for service personnel. The vast majority of American losses date from World War II. Research for family members of servicemen in World War II and the Korean conflict is especially dependent upon access to DMF/SSDI. Many servicemen from this time period were born prior to state vital records, as certainly were their parents. With the mass migrations during the 1930s, 1940s, and to some extent the 1950s, DMF/SSDI is very often the only resource that military contract genealogists have to trace relatives whose **genealogy** is vital to identifying family members eligible to submit DNA Family Reference Samples. Department of Defense currently estimates that 83,000 Americans are unaccounted-for from World War II, the Korean War, the Cold War, the Vietnam War and the 1991 Gulf War.[2] Our government, our citizens, the families, and our service personnel rely upon the services of **genealogists** to accomplish the missions of the Defense Department and the casualty divisions of each of the military branches.
- Organizations which work with coroners to find the families of unclaimed service personnel and other deceased persons depend upon **genealogical** research to solve these cases.
- The DMF/SSDI is a vital tool among legal professionals, especially in probate and other cases which involve proving heirship. In states with closed death records and no published death indexes, the DMF/SSDI may be the only resource for tracing and proving heirship. In closed records states, the DMF/SSDI record may be the only source available that meets evidentiary rules for admissibility for documenting deaths to the satisfaction of the court.

- Title companies, oil/gas and mineral companies use the DMF/SSDI for the same reasons. When oil companies cannot trace and identify lineages from original mineral owners, the unknown heirs cannot be identified. In these cases, courts often issue orders allowing drilling and production. Heirs to the mineral rights are in effect cheated out of their economic benefit.
- Next of kin in guardianship cases, youth transitioning from foster care, adoption require

[2] Defense Prisoner of War, Missing Personnel Office (http://www.dtic.mil/dpmo/ : accessed 15 February 2012)

genealogical kinship determination.

- Capital mitigation in death sentence cases relies upon **genealogical** reports among others submitted for consideration by the court.
- **Genealogical** research and facts are often used in immigration and citizenship cases to prove or disprove citizenship or residency.
- Determination of heirs to civil pension, Social Security, and veteran's benefits depends on **genealogical** research.
- Identification of next of kin prior to cemetery removal is mandated in many states. This may involve **genealogical** research over several generations.
- Provenance, class action claimants, intellectual property-rights cases may also heavily depend upon **genealogical** research.

On 15 February 2012, Council for the Advancement of Forensic Genealogy polled a dozen of its associates, asking for a description of the usage of the DMF/SSDI in just *one* recent case that each has worked on:

> **Tina S. in Tennessee** - Intestacy case for estate valued at $200,000 in which DMF/SSDI was the sole source for proof of death for thirteen maternal aunts and uncles.
>
> **Connie S. in North Carolina** - Korean War MIA case in which DMF/SSDI was accessed for both his parents, three of his four sisters and their husbands, five paternal uncles and their wives, one maternal aunt and spouse, and five maternal uncles and spouses as well as some of the children of these persons. DMF/SSDI accessed 25-30 times for this one case.
>
> **Catherine D. in Vermont** - Army repatriation case, accessed DMF/SSDI approximately 12 times in a search for siblings, half-siblings, parents, aunts, and uncles.
>
> **Michael R. in Pennsylvania** - Adams County intestate estate that had 22 citations to different persons' DMF/SSDI records (out of 154 citations). These helped find all 26 first cousins once-removed - all of whom will share in the estate.
>
> **Michael H. in Delaware** - National Park Service, at Monocacy National Battlefield (Frederick, Md.). Used the DMF/SSDI multiple times to determine date and place of death of descendants of former slaves who were owned and lived on this plantation. When no other death record could be obtained, the DMF/SSDI record was cited 7-9 times as proof of death.
>
> **Janice S. in California** - Heir search case for property to be sold, tracked forward three generations, multiple children in each generation, used DMF/SSDI for about 20 individuals in the case.
>
> **Kelvin M. in Texas** - Probate case where the decedent was only child, her parents were only children, so case goes back to the great grandparents. At present, 172 heirs identified and used DMF/SSDI multiple times daily for this case.
>
> **Leslie L. in Oregon** - Quiet title, bank needs to foreclose on estate but first needs to identify heirs. Accessed DMF/SSDI 7-8 times during initial stage of research.
>
> **Claudia B. in Washington state** - Working with a local police department to identify the family of a woman whose ashes were found in abandoned storage unit. Accessed

DMF/SSDI 7 times for the deceased, her husband, their three children and daughter- and son-in-law.

Dee Dee K. in Texas - Capital mitigation in a death penalty case, **genealogical** research over three generations, accessed DMF/SSDI 22 times. (Ms. King has provided the Department of the Navy Casualty POW/MIA Branch with Family Reference Sample donors on 279 cases. Her genealogical master database shows more than 3,000 citations to DMF/SSDI during the course of that research.)

Liesa H. in Massachusetts - Pro bono case, attempting to reunite a Vietnam veteran with the surviving family of another veteran who died in his arms. The veteran has wanted to speak to the family of his fallen colleague for more than 40 years. DMF/SSDI accessed 4 times during initial stage of research.

Barbara S. in Georgia - Georgia estate and have thus far used the DMF/SSDI 36 times. One living first cousin in her 90s and several first cousins once removed have been identified.

Council for the Advancement of Forensic Genealogy respectfully requests that the Committee please consider measures that will help the DMF/SSDI meet the potential it was designed for - to *prevent* identity theft. Loss of public access to this irreplaceable resource will have NEGATIVE financial, legal, and other impacts.

Name: Charlene M. Pipkin
Address: 328 South 900 East, Orem, UT 84097
Phone Number: 801-225-5370
Email: genealogyguide@ymail.com
Title of hearing: Hearing on Social Security's Death Records

I appreciate the opportunity to provide my perspective on the accuracy and uses of the Social Security Administration's Death Master File.

If my understanding is correct, the information in the Death Master File is used by government agencies, financial institutions, medical and genealogical researchers, and workers' benefit plans to prevent fraud, waste, and abuse. As a genealogist, I use the Death Master File to help clients find correct information about their deceased ancestors. This often leads to filing a request for the SS-5 (application) form, which might provide genealogical information not available elsewhere. Many of my clients have personal reasons for learning about their ancestry. Some have legal and medical reasons for doing so. The closing of the Death Master file impacts my legitimate research.

According to the information posted on your website (http://waysandmeans.house.gov/News/DocumentSingle.aspx?DocumentID=276834), of the 2,500,00 deaths reported each year, 14,000 individuals are incorrectly listed on the Death Master File. Although it is regrettable that even one death is reported incorrectly, this is a "fail" rate of about .5%. Only a portion of that .5% results in personal and financial hardship for those who are erroneously listed as deceased and a smaller portion results in identity theft. All systems will have inefficiencies, but I believe that the benefits of making the Death Master File public outweigh the risks and that other means can be found for dealing with misinformation rather than closing the Death Master File.

Thank you to the Subcommittee on Social Security for allowing me the opportunity to make this statement. I am making this statement on behalf of my own interest and not as a representative of clients or any other group.

Sincerely,

Charlene M. Pipkin, Accredited Genealogist®

Gentlemen;
I noted that you did not have any representation from genealogists among your people selected to testify.
You must realize by now that any well intentioned attempt to block access to the social security death index will NOT deter criminals from gaining information from which they can steal identities.
The impact upon genealogists both professional and amateur will be profound. This index is invaluable in searching for ancestors and gaining family information.
Please do not overlook the unintended consequences of any action that you may take.
Thank you.

Charles E. Green
4560 Terrasanta
Pensacola, FL 32504
850-479-8235

February 3, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Although the hearing on this matter was scheduled for yesterday, February 2, I still wish to submit these comments for the record.

I support Congress's intent to protect Americans from improper usage of our personal information, and to help protect us from identity theft. However, I oppose restriction of access to public records rarely related to identity theft.

Currently, four bills are pending in the Congress that would eliminate or curtail access to the Social Security Death Index on the Internet:

> **HR 3475**, *Keeping IDs Safe Act of 2011*
> If enacted, this bill effectively ends public access to the SSDI/Death Master File.
>
> **S 1534**, Identity Theft and Tax Fraud Prevention Act
> **HR 3482**, To prevent identity theft and tax crimes
> **HR 3215**, To prevent identity theft and tax fraud
> If enacted, these bills prohibit disclosure of a deceased's Social Security Number in calendar year of death and calendar year following death.

I oppose these bills for the following reasons:

Access to the SSDI/Death Master File:

1. Does not lead to a significant proportion of identity theft.
   The vast majority of identity theft occurs, instead, from computer security breaches of institutions and enterprises holding records of *living* individuals.
2. Helps to *prevent* identity fraud.
   Access allows verification of a person's death and thereby helps to prevent fraud (per the National Technical Information Service (NTIS) website).
3. Is vitally important to the work of genealogists such as myself.
   We rely heavily on these records when doing US research both in and outside the United States. Their importance to our research cannot be overestimated.

For these reasons, I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Respectfully,

Christine T. Rauckis
992 Woodington Road
Westerville, Ohio 43081

2/2/2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Christopher Cowan
12118 Walnut Park Xing Apt 934
Austin, TX 78753

HR 3475
Please stop our kids from being targeted by identity thieves who are abusing the master death file. Parents of children passed should not have to go through this.
Thank you,
Christy Bergen
35404 26th Ave S
Federal Way, WA 98003
253-350-4845
Christybergen@live.com
HR 3475

Dear Chairman Johnson and Members of the Committee:

RE:
• HR 3475, Keeping IDs Safe Act of 2011
• S 1534, the Identity Theft and Tax Fraud Prevention Act
• HR 3482 To prevent identity theft and tax crimes.
• HR 3215 To prevent identity theft and tax

I am writing to urge that you consider the economic and other ramifications that these proposals will have upon commerce, the legal community, and governmental activities.

Public access to the **Death Master File, Social Security Death Index (SSDI)** is an irreplaceable resource used across the commercial spectrum as well as by attorneys, bank and trust companies, title companies, oil and gas companies, medical researchers, forensic genealogists, and others. Human resource departments large and small use the SSDI as part of their compliance with federal hiring guidelines. A few additional examples are below.

The Department of Defense is mandated by Congress to repatriate the remains of our unaccounted-for service personnel. The vast majority of American losses date from World War II. Research for family members of servicemen in World War II and the Korean conflict is especially dependent upon access to SSDI. Many servicemen from this time period were born prior to state vital records, as certainly were their parents. With the mass migrations during the1930s, 1940s, and to some extent the 1950s, SSDI is very often the only resource that military contract genealogists have to trace relatives whose genealogy is vital to identifying family members eligible to submit DNA Family Reference Samples. These facts also apply to those organizations who work with coroners to find the families of unclaimed service personnel and other deceased persons

The SSDI is a vital tool among legal professionals, especially in probate and other cases which involve proving heirship. In states with closed death records and no published death indexes, the SSDI may be the only resource for tracing and proving heirship. In closed records states, the SSDI record may be the only source available that meets Rules of Evidence for documenting deaths to the satisfaction of the court. Title companies, oil/gas and mineral companies use the SSDI for the same reasons. When oil companies cannot trace and identify lineages from original mineral owners, the unknown heirs cannot be identified. In these cases, courts often issue orders allowing drilling and production. Heirs to the mineral rights are in effect cheated out of their economic benefit.

I am a certified genealogist accredited by the Board for the Certification of Genealogists and I work as a contract genealogist in the area of forensic genealogy where it is vital to have access to the Death Master File/Social Security Death Index in order to trace the living heirs of soldiers missing from WWII, Korea and Vietnam. Removal of access to this source will greatly impact my ability to render this service for our missing soldiers.

This is just a small example of how many in the commercial, business, legal and governmental communities rely upon the irreplaceable SSDI. Please consider measures that will help the SSDI meet the potential for which it was designed - to *prevent* identity theft. Loss of public access to this irreplaceable resource will have NEGATIVE financial, legal, and other impacts.

Constance T. Shotts, Ed.D., CG(sm)
104 Locust Run Place
Monroe, NC 28110
704-283-7249
cshotts1@carolina.rr.com

Connecticut Professional Genealogists Council, Inc.
P. O. Box 4273
Hartford, Connecticut 06147-4273
08 February 2012

Re: Hearing on Social Security Death Records

To Members of the Subcommittee:

We are opposed to the closing of the Social Security Master Death File. It was created to prevent the types of misuse that speakers at your hearing described.

Financial institutions, the Internal Revenue Service and other entities that use the Social Security number for identification need to improve their procedures for detecting fraudulent use of the numbers. The Social Security Administration needs to create a system for ensuring that individuals are actually deceased before they are listed in the Master Death File. We feel that these issues can be resolved with a minimum of effort. Closing the File to the public will not resolve these issues.

The Social Security Master Death File is an important tool in our work. Closing the database will have a negative effect on our ability to conduct our businesses, and will cause us economic hardship. A short and incomplete list of how we use this database includes

identifying lawful heirs in probate cases
identifying relatives of military personnel who have been missing-in-action and whose remains have been found
identifying relatives of people who need to understand the genetic basis of their medical conditions

There are compromises that can be considered as alternatives to closing the Social Security Master Death File to the public. These could include

not listing deceased children until the date of their 18th birthday
not listing deceased individuals for one year after their death
listing individuals immediately but not listing their Social Security numbers for one year

Our position was not represented in the testimony of invited speakers at the hearing on this topic. We ask that you consider our position and recognize the importance of this database to the American people and to the people who use the Master Death File for legitimate business purposes

Sincerely yours,
Nora Galvin, President
representing the 56 members of the
Connecticut Professional Genealogists Council, Inc.
Hartford, Connecticut
(203)-362-2232
auntlizzie@snet.net

February 1, 2012

House Ways and Means
Washington, D.C.

Dear Committee,

I am writing to you in regards to the Social Security Death records legislation. I am the C.E.O. of a company in California that conducts genealogy research for missing heirs of estates. Our business and ability to locate individuals would be greatly impacted should this measure pass and the access to records be blocked.

Our business is but one example of the thousands of small business that were created from scratch and an idea many years ago. This is what America stands for. In the current climate of unemployment and businesses failing, this is not the time or reason to place additional limitations and restrictions on those that employ people and contribute to the economy in so many ways.

If this measure passed, the lives and livelihood of thousands of individuals are at stake. The SSDI records that we as business individuals currently access and rely on cannot be taken away. I could compile a list of hundreds of average citizens whose lives were changed because our company located them and through information taken from the SSDI determined they were entitled to financial assets from a deceased relative.

Please take in all the evidence submitted and pray on the matter before a decision is made to shut down this valuable resource.

David B. Hogan
Kendra Asset Recovery Inc.
28020 Durham Place
Santa Clarita, California 91350
Kendra@socal.rr.com
Social Security Death Records Legislation

As a professional genealogist, I am very disturbed at the possibility of permanently abolishing access to the Social Security Death Index. Because many states won't release death records for many years following a person's death, the Social Security Death Index is a prime source for genealogists to access this important vital information. I realize that there is some concern over identity theft and the illegal use of Social Security numbers but the death index could be made available without including a social security number. I hope the committee will give professional genealogists a chance to comment on this in person. Thank you for your time.

Debbie Gurtler

Professional genealogist

949 N. Fox Hollow Drive

North Salt Lake, UT 84054

801-372-7785

dsgurtler@gmail.com

Social Security Death Records

Dee Dee King
Certified Genealogist℠
Forensic Genealogy Services, LLC
PO Box 1085, Manvel TX 77578
telephone/fax 281.431.3525
email king@ForensicGenealogyServices.com

16 February 2012

Dee Dee King, Certified Genealogist,
Forensic Genealogist
Contract Genealogist for the Navy POW/MIA Branch, Casualty Department
PO Box 1085
Manvel TX 77578
281-431-3525
King@forensicgenealogyservices.com

Chairman Johnson Announces a Hearing on Social Security's Death Records
Submission for the record: waysandmeans.submissions@mail.house.gov

I am a forensic genealogist. My job is to document kinship determinations for cases with legal implications. These cover a wide range of possibilities:

- Probate and estate cases - known heirs, unknown heirs, missing heirs.
- Heirs and beneficiaries of trust and insurance accounts.
- Due diligence affidavits.
- Next of kin in guardianship cases, youth transitioning from foster care, adoption.
- Capital mitigation in death sentence cases.
- Immigration and citizenship cases.
- Civil pension, Social Security, and veteran's benefits.
- Land issues involving title, adverse possession, rights of way, *lis pendens*, or muniment of title.
- Oil, gas, and mineral royalties.
- Identification and location of next of kin or DNA donors in matters involving unclaimed decedents or POW/MIA personnel repatriation.
- Identification of next of kin prior to cemetery removals.
- Provenance, class action claimants, intellectual property-rights.

In many of these cases I am either appointed by courts or hired by attorneys to conduct this genealogical research. I also serve as the contract genealogist for the US Navy Casualty POW/MIA Branch. My job there is to research and document kinship in order to identify and

locate those eligible to contribute DNA Family Reference Samples to aid in the repatriation of remains of our unaccounted-for Navy servicemen.

I could NOT effectively conduct this vital genealogical research in these cases without access to the Death Master File, Social Security Death Index (SSDI). Research in many of the cases mentioned above must extend back before state vital records were mandated. Most states have closed public records. Many do not publish death indexes. SSDI is an **irreplaceable** resource.

The Department of Defense is mandated by Congress to repatriate the remains of our unaccounted-for service personnel. The vast majority of American losses date from World War II. Research for family members of servicemen in World War II and the Korean conflict is especially dependent upon access to SSDI. Many servicemen from this time period were born prior to state vital records, as certainly were their parents. With the mass migrations during the 1930s, 1940s, and to some extent the 1950s, SSDI is very often the only resource that military contract genealogists have to trace deceased relatives. This genealogy is vital to identifying family members eligible to submit DNA Family Reference Samples.

These facts also apply to those organizations which work with coroners to find the families of unclaimed service personnel and other deceased persons.

This also applies to many probate cases in which intestate decedents were quite elderly, many times with parents born in the late1800s. I am required to submit reports that meet the Rules of Evidence in Texas courts. When state death records are closed to me, the only alternative is to produce and document evidence of a death from the SSDI. If that resource is made unavailable, I will have nothing to rely upon in its place.

My company is a small, woman-owned, and Vietnam veteran-owned business. Subscription directly through the Social Security Administration for access to the SSDI is exorbitant beyond our means. The loss of public access to the SSDI will have one or all of the following effects:

- Cause such extended research for alternative documentation that my rates become exorbitant;
- Further burden the stretched budgets of legal jurisdictions and the military branches;
- Result in failed research and documentation.

Please work with the public to find ways to help protect the privacy of the living while keeping this vital record of deaths available for legitimate use. Please hold the Internal Revenue Service accountable for the proper use of the SSDI in preventing identity theft and fraud with improper use of Social Security numbers.

Doris Roden
Brookings Area Genealogical Society
727 Main Avenue
Brookings, South Dakota
jdroden@brookings.net
HR 3475, Keeping IDs Safe Act of 2011

As a hobby, but trained, genealogist, I use the SSDI frequently for my own family research and to help others find their ancestors.

I grew up not knowing my grandparents. Since my retirement in 2008, I have been researching my family history and, because of it, have developed a greater appreciation and understanding for my parents and ancestors.

As president of our local genealogical society, I work with our board and members to help others trace their family histories. Please do not take these important research tools away from us.

Please vote against passage of this bill and advocate its defeat in the subcommittee.

U.S House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Federation of Genealogical Societies
Linking the Genealogical Community

Statement for the Record

Hearing on Social Security's Death Records

Submitted by

Patricia A. Oxley, President

February 2, 2012

Chairman Johnson, Ranking Member Becerra, and members of the Subcommittee.

Thank you for the invitation to submit this Statement for the Record on behalf of the Federation of Genealogical Societies to supplement the record of the hearing held by the Subcommittee on the 2nd of February 2012.

I serve as the President of the Federation of Genealogical Societies and as a member of the Records Preservation and Access Committee more fully described below.

The Federation of Genealogical Societies was founded in 1976 and represents the members of hundreds of genealogical societies. We have member societies in all 50 states, the District of Columbia, the Virgin Islands, Canada, Ireland, and the United Kingdom.

Be assured that the genealogical community shares the objective of protecting Americans against fraud and of addressing deficiencies in the current operation of the Social Security Administration's Death Master File. This hearing marks our first opportunity to express our views to Congress on this important subject and we commend the committee for adding it to their agenda.

Identity Thieves Have Long Targeted Infants

We have all been outraged by reports of identity thieves filing fraudulent tax refund claims using the SSNs of recently deceased infants & adults. Although the specific techniques and technologies may have changed, having a scoundrel target deceased infants is not new.

In the 1970s and early 1980s, the technique followed by those with sinister intent employed this pattern:

(1) The thief would visit the Babyland Section of a local cemetery and find the name and birth date of a deceased child roughly comparable with their own.

(2) The thief would approach the vital records custodian to request a duplicate birth certificate using that name and birth date.

(3) If issued, the duplicate birth certificate would then be used to apply for a driver's license and other purposes to create an identity in the deceased child's name that could then be used for purposes as benign as facilitating underage drinking but ranging to major thefts by making substantial credits purchases.

What Response Worked

The most effective response developed by the vital records community to this abuse was to verify the appropriateness of the request for a duplicate birth certificate by first checking their files of death certificates to ensure that the subject of the requested birth certificate was not found

there. If found, the duplicate birth certificate would only be issued if prominently annotated to reflect the fact that the person was deceased.

Inter-state compacts with adjoining jurisdictions allowed the vital records custodians of the birth records to screen the death records of neighboring states before responding to a fraudulent request. Efforts continue to expand the ability to access the death records of a broader range of states to be used to thwart this form of abuse.

As a society, we did not choose to restrict access to cemeteries.

What Is the Problem?

Death records have particular utility in the prevention of fraud or theft. Little judgment is required to decide not to extend credit to a person authoritatively reported to be dead.

That reality places a particular burden on those creating such a record to get it right and a requirement to correct any mistakes as quickly as possible.

Thieves may be abusing online access to the Master Death File or its commercial form, the Social Security Death Index.

The real problem is that the Internal Revenue Service and others, who should be using it for the purpose for which it was created are not!

About the Records Preservation and Access Committee

The genealogical community works together through The Records Preservation and Access Committee (RPAC), a joint committee which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS) and the International Association of Jewish Genealogical Societies (IAJGS) as voting members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), the American Society of Genealogists (ASG), and industry representatives also serve as participating members. RPAC meets monthly, and more often if needed, to advise the genealogical and historical communities, as well as other interested parties, on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

Summary

The most effective response to identity thieves' abuse of vulnerabilities in the online tax refund system is to use the Master Death File for the purpose for which it was originally created, namely, fraud prevention.

Title of Hearing:
Hearing on the accuracy and uses of the Social Security Administration's Death Master File scheduled for 2 February 2012.

FOCUS OF THE HEARING
The hearing will focus on the history, accuracy, use and impacts of the Death Master File along with options for change.

I am writing in reference to the hearing on the Social Security Administration's Death Master File scheduled for 2 February 2012. I understand that the issue at hand is the privatization of these records in order to protect the privacy of individuals and help prevent the fraudulent use of social security numbers. I am writing to request your support in the opposition of this action.

As a Landman researching title in the oil and gas industry for Marcellus Shale here in Pennsylvania and West Virginia, I frequently had to find heirs to mineral rights as a pre-requisite to leasing. The SSDI was of enormous help in constructing a genealogy tree to ensure we were on the right track to finding the correct property owners. I cannot imagine the nightmare of not having access to the SSDI to complete my work assignments.

Additionally, I am a member of the Unclaimed Persons volunteer genealogy group. Our purpose is to volunteer our expertise to find the next of kin for persons who have died so that their remains can be claimed for burial. If that can be accomplished, the local government does not have to bear the costs of burial. We do a lot of work for the Hillsborough County, Florida, Pottawattamie County, Iowa and Orange County, California, Coroner's Offices, and are starting to do work for other offices around the country due to our success rate. Often, the only starting information we have is a social security number, which tells of a date and state of issue, and birth date, all of which are invaluable in a search for next of kin. Since we are volunteers, this costs the county governments nothing.

Finally, as a genealogist for my own and others' family trees, I would simply be lost without the birth and death dates in the SSDI. I certainly would be chasing down many dead ends. I couldn't tell you how many people I've found due to clues from the SSDI.

Surely there must be another solution other than privatizing the Social Security records. Perhaps something as simple as marking an inactive number with an "*" so that it will not recognize someone trying to use the number for a fraudulent purpose would work. I just cannot believe that in today's technological world we can't find some way to do this. My personal belief is that we should not be using SS numbers for identification. I would rather see a national ID card!

In closing, please consider opposing the privatization of the Social Security Death records. I truly believe that there is another way to prevent fraud.

Regards,

Name: Florence R. Stoneberg
Organization (if applicable): Unclaimed Persons
Address: 104 Driftwood Drive, McMurray PA 15317-6630
Phone Number: 724-941-5522
Contact E-mail Address: fstoneberg@yahoo.com

Feb. 4, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to do with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Frances Neuvirth
289 Hurd Street
Milan, MI 48160
734 439-7607
n_Fran@hotmail.com

Frederick C. Hart, Jr.
Certified Genealogist[SM]
Fellow of the American Society of Genealogists

1311 Great Hill Road
North Guilford, CT 06437-3649
203-457-9383 □ Hartfc@aol.com

31 January 2012

Subcommittee on Social Security
Ways and Means Committee
US House of Representatives
Washington, DC
(sent by email attachment)

Ladies and Gentlemen,

I write to urge you to keep the Social Security Death Master File available for public access for important legitimate purposes, such as genealogy, heirship determination, and family medical history. I write from the perspective of a professional genealogical researcher with over 25 years experience who is also a Certified Genealogist,[SM] a fellow of the American Society of Genealogists, and an active member of several regional and local genealogical and historical societies.

In my opinion, the Death Master File is a resource intended to help **prevent** identity fraud, not to facilitate it. Closing its availability to legitimate uses will have no beneficial effect and will only prevent those legitimate users, including myself, from making the proper relationship determinations that are essential to their genealogical or family history endeavors. I heartily endorse the comments provided by the Records Preservation and Access Committee in their draft document of 24 January 2012.

I appreciate your consideration of these comments. I am representing myself in this letter and my personal contact information is in the above header. I am also an active member and/or associate of the following organizations:

Board for Certification of Genealogists (associate)
American Society of Genealogists (fellow)
Connecticut Professional Genealogists Council (member)
New England Historic Genealogical Society (member)
New York Genealogical and Biographical Society (member)
Connecticut Ancestry Society (member)
++ Numerous other local historical and genealogical societies

Sincerely,

Frederick C. Hart Jr., CG, FASG

These are written comments associated with the February 2, 2012 Hearing on Social Security's Death Records. They are justification for retaining the SSDI information on the Internet and readily available to citizens. I am a strong advocate for protecting privacy, but in this case the advantages of retaining the SSDI information on the Internet far outweigh the disadvantages.

- Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft.

- Rarely, has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen"[1]. Many of these computer breaches have been well documented in the press.[2]

- Genealogists doing US research located both in and outside the United States, rely on the Social Security Death Index (SSDI), which is the commercial name of the Death Master File (DMF). The Death Master File is a computer database file made available by the United States Social Security Administration since 1980.

- SSDI is a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (http://www.ntis.gov/products/ssa-dmf.aspx), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. In addition to family history researchers, the SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

- Genealogy is a hobby for millions of people.
  A study from May 2009[3] characterizes those individuals interested in genealogy as follows:
  49 million feel a deep appreciation for their ancestors*
  13 million are active researchers**
  More than 8.5 million visited genealogy-oriented sites in the last month (excluding search engines and long-tail sites).***
  9 million are hobbyists**
  1.6 million online adults 18-44 consider genealogy a hobby (3%)
  7.5 million online adults 45+ report genealogy a hobby (8%)
  A total of 9.1 million total hobbyists (out of an online universe of 148 million 18+)

- Genealogy also is a serious profession.

- Genealogists use the SSNs to appropriately identify records of people when tracing family medical history, especially if the person has a common name: Sara Cohen, Tom Brown, Jose Martinez, Trung Lee, etc. Genealogy assists in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The SSN is critical to make certain that one has the correct person. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family[4]. Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative[5].

- Genealogists work with coroners to find next of kin for the deceased. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See www.unclaimedpersons.org

- Genealogists work with military to locate relatives of soldiers who are still unaccounted for from past conflicts. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family. [6]

- Other stakeholders who are concerned and want full and immediate access to the SSDI include: the financial and insurance industries [they need the information timely so that they can verify deaths to pay out death claims and verify beneficiaries for paying retiree benefits]; federal, state and local law enforcement agencies; Lexis-Nexis; charities legacy departments and planned gifts departments, medical researchers [tracking morbidity cluster deaths and tracking mortality of medical trial results]; state, county government and teacher retirement funds; county assessment offices, student loan companies; universities for student loans, tracing alumni mortalities and

other activities, enhanced collections department of state courts, and other stakeholders that we are learning about daily.

---

1. http://www.identitytheft.info/breaches09.aspx
2. http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer_breach/
   http://www.nctimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html
   http://www.qctimes.com/news/local/article_06d38e24-146a-11df-91c6-001cc4c03286.html
3. *MRI, May 2009 "Respect for ancestors is very important", **@Plan, May 2009 "Researched family history online in last 30 days" and "Hobbies = genealogy", ***Comscore Media Metrix, Mar 2009, Heat maps are @Plan, May 2008
4. Mayo Clinic staff: "Medical History: Compiling your medical family tree"
   http://www.mayoclinic.com/health/medical-history/HQ01707;
5. https://familyhistory.hhs.gov/fhh-web/home.action
6. http://www.aarp.org/relationships/genealogy/info-06-2011/genealogy-tips.html

Name: Victoria P. Scott

Organization: Genealogy Research of North Carolina

Address: 229 Danagher Court, Holly Springs, NC 28540

Phone Number: 919-880-6231

Contact E-mail Address: victoria.p.scott@gmail.com

Title of Hearing : **Chairman Johnson Announces a Hearing on Social Security's Death Records**

Dear Senators:

Please do not restrict or close the Social Security Death Index from public access. Many states (including North Carolina, where I reside) have public indexes, with links to copies of the original underlying public vital records. This allows individuals the means to document their own personal history.

In North Carolina, for instance, **all** birth, marriage, and death records are **public documents**. Death certificates, which can be accessed online instantly through fee-paid entities (ie/ Ancestry.com and Archives.com), or obtained in person at the North Carolina Department of Health and Human Services, have the deceased individual's Social Security number displayed.

North Carolina is the 10th most populated state, and is not alone in recognizing that citizens have the right to access personal identifying information. The SSDI allows individuals to obtain this information regardless of an individual's last place of residence. Closing the SSDI will impact my ability to assist a client in tracing their family history.

Once again, please keep the SSDI a matter of public record.

Respectfully submitted,

Victoria P. Scott
Genealogy Research of NC
229 Danagher Court
Holly Springs, NC 27540
(919)880-6231
http://www.amazon.com/shops/A8DNPXAPIJ3OH
www.ncgenealogy.net

waysandmeans.submissions@mail.house.gov

Name Hallie P. Garner

Organization (if applicable)

Address 8923 Woodshore Drive, Dallas, TX 75243

Phone Number 214-349-3869

Contact E-mail Address hallie.garner@sbcglobal.net

Title of Hearing Chairman Johnson Announces a Hearing on Social Security's Death Records Feb 02, 2012

I would like to advocate against restricting access to the Social Security Death Index (SSDI). I am a genealogist and have found the SSDI invaluable in helping me determine what happened to my family members. **If I have the date they died and where they last lived, I can then use that information to locate an obituary or a cemetery location**.

In this age when families have become so widespread, it is hard to know where people went when they left their home area, and the SSDI has helped me thousands of times with finding locations. The SSDI doesn't give enough information for people to use it for voter fraud, but there are lots of OTHER sources out there that do. It does not provide addresses which are needed for voter fraud.

Please do not stop access to this very valuable source of information for genealogists.

Sincerely yours,

Hallie Garner

Helen Schatvet Ullmann
Certified Genealogist; Fellow of the American Society of Genealogists
713 Main St., Acton, MA 01720
978-263-2037
hsullmann@comcast.net

Re: Hearing on Social Security's Death Records

I am concerned that the Social Security Death Index online at many sites, may be limited in scope and/or that it may no longer be available to family historians or genealogists.

This index is a wonderful tool for those seeking to compile information on their families, or on clients' families. The deaths of many people born in the 19th century appear in this index.

I cannot see any reason to limit the distribution of this information. In fact, the more widely it is available, the more difficult it would be for anyone seeking to use a person's identity fraudulently.

Please do not limit access to this source.

International Association of Jewish Genealogical Societies (IAJGS)
6052 Hackers Lane Agoura Hills, CA 91301
818-889-6616 tel 818-889-0189 fax
www.iajgs.org

STATEMENT FOR THE RECORD, HOUSE COMMITTEE ON WAYS AND MEANS, SUBCOMMITTEE ON SOCIAL SECURITY, WRITTEN COMMENTS ON PROVISIONS RELATING TO SOCIAL SECURITY ADMINISTRATION'S DEATH MASTER FILE, ALSO KNOWN COMMERCIALLY AS THE SOCIAL SECURITY DEATH INDEX.

I. INTRODUCTION:

The House Committee on Ways and Means, Subcommittee on Social Security, held a Hearing on 2 February 2012, regarding the accuracy and uses of the Social Security Administration's Death Master File. The genealogical community was informed that no invitation to testify at the hearing would be forthcoming, but that we – the genealogical community – were invited to submit a statement. This statement is accordingly submitted.

II. IAJGS BACKGROUND & CONTACT INFORMATION:

The International Association of Jewish Genealogical Societies is the umbrella organization of 70 genealogical societies and Jewish historical societies worldwide whose approximately 10,000 members are actively researching their Jewish roots. We want to ensure that our members will be allowed continued and maximum access to these vital records. The IAJGS and its predecessor organization were formed in 1988 to provide a common voice for issues of significance to its members and to advance our genealogical avocation. One of our primary objectives is to promote public access to genealogically relevant records. In 2012, we are holding our 32nd consecutive annual International Conference on Jewish Genealogy (www.iajgs.org).

Contact Information:
IAJGS official mailing address is:
IAJGS
PO Box 3624
Cherry Hill, NJ 08034-0556

However, for purposes of this statement please use the following contact information:

Jan Meisels Allen,
Vice President, IAJGS
6052 Hackers Lane
Agoura Hills, CA 91301
(818) 889-6616 tel (818) 991-8400 fax (call before submitting a fax)
e-mail: vicepresident@iajgs.org

Thank you for the opportunity to present the IAJGS concerns regarding the Subcommittee's proposed elimination or reduction of public access to the commercial version of the Death Master File (DMF), the Social Security Death Index (SSDI). For the purposes of this statement, we will be addressing access to the SSDI rather than the DMF, as the SSDI is the version that genealogists are permitted to access. We were surprised and disappointed that the genealogical community was not invited to participate at the February 2nd hearing. The genealogical community, an important stakeholder in the proposed legislation, had been working tirelessly with the Subcommittee staff since mid-November – providing information on genealogists' use of the SSDI and suggesting legislative language to deter identity theft while retaining public access.

It is ironic that a system that is used to prevent identity theft (by permitting employers, financial organizations, insurance companies, pension funds, and others the ability to check names against those deceased as reported on the Death Master File), [http://www.ntis.gov/products/ssa-dmf.aspx] is now being determined—inappropriately—as an instrument of identity theft.

We support the Subcommittee's intent to protect the residents of the United States from improper usage of their personal information, and to protect them from identity theft. But, rarely has it been documented that an individual's identity is violated by access to vital records or the SSDI; rather, the violations occur due to computer breaches from government and private enterprises. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen"[1]. Many of these computer breaches have been well documented in the press.[2]

Genealogists Are Not the Cause of Identity Theft

We watched the February 2nd hearing and were disturbed by some of the misinformation and inferences that were given during the hearing. **Genealogists are not the cause of identity theft.** Thieves are the cause of identity theft. Financial institutions and government agencies have been hacked into numerous times and that has been documented [1, 2], but was not mentioned during the hearing. Nor was there mention of returning to using non-computerized data to avoid the inevitable hacking that occurs daily in the 21st century. If we accept the continued use of computerized data, and the continued likelihood of hacking occurring to any given database at any time, then we must also accept that, occasionally, misuse of data will occur. It is not reasonable, Constitutional, or in the Nation's interests, to remove public documents from public access. For a real solution to this problem, see below "IRS Needs to be More Proactive."

As parents and grandparents there is nothing that we can adequately express to Mr. Agin, his wife, and the other parents of deceased children about their grief over the agonizing loss of their children. With all due respect, do we know for a fact that Mr. Agin's daughter's Social Security number was taken from the public SSDI?

Mr. Agin, in his reply to Chairman Johnson's question asking just that, said "**it was his personal belief** that someone who trolled blogs about sick children and then used the access of the SSDI on genealogical websites". He stated, while it was possible, he would like to believe it was not the case, that it was someone involved with the medical institutions where his daughter was treated--as they would have access to her Social Security number**. Neither the assumption that it was taken from a genealogical website or that his daughter's Social Security number was not stolen from one of the medical institutions where his daughter was treated are based on facts.** Unfortunately, medical identity theft, whereby medical employees have been found to steal patient's identification has become a growing business.[3]

Mr. Agin mentioned that 14 other parents of children who died from cancer reported that their children were also victims of identity theft. As noted above, many government and financial institutions have been victims of computer hacking and many hospital employees have been found to steal patients' Social Security Numbers. It is remarkable that the cancer victims were targeted—as the SSDI does not include cause of death. Therefore, it is equally possible that the Social Security number was stolen

from the medical institution, provider's office or an off-site medical records subcontractor by an individual or a computer hacker.

Removal of the SSDI from public access would not necessarily reduce the problem of fraudulent use of a Social Security number. As it will no longer be available as a reference check to many who use it as an identity theft deterrent, it may well increase identity theft.

Interest in Family History/Genealogy

Millions of Americans are interested in their family history; The Harris Interactive Poll taken in August 2011 found that four in 5 Americans have an interest in learning about their family history. The Poll also reported 73% of Americans believe it is important to pass along their family's lineage to the next generation.[4] Genealogists doing U.S. research located both in and outside the United States rely on the Social Security Death Index.

Family Medical History

Genealogists use the Social Security Numbers (SSNs) to appropriately identify records of people when tracing **family medical history**, especially if the person has a common name: Sara Cohen, Tom Jones, Jose Martinez, Mary Smith etc. During the hearing, Mr. Pratt, representing the Consumer Data Industry Association (CDIA), mentioned CDIA had conducted a study and found some people with common names, i.e. Smith, also had the same last four digits on their Social Security number, validating why the complete Social Security number is necessary.

Genealogy assists researchers in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The SSN is essential to make certain that one is researching the correct person. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family [5]. Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative[6].

There are many genetically inherited diseases, but for the purposes of this statement, we will mention the *BRCAI* and *BRCA2* genes' mutations and breast and ovarian cancer. The following information is from the National Cancer Institute [7].

> "A woman's risk of developing breast and/or ovarian cancer is greatly increased if she inherits a deleterious (harmful) *BRCA1* or *BRCA2* mutation. Men with these mutations also have an increased risk of breast cancer. Both men and women who have harmful *BRCA1* or *BRCA2* mutations may be at increased risk of other cancers.
>
> The likelihood that a breast and/or ovarian cancer is associated with a harmful mutation in *BRCA1* or *BRCA2* is highest in families with a history of multiple cases of breast cancer, cases of both breast and ovarian cancer, one or more family members with two primary cancers (original tumors that develop at different sites in the body), or an Ashkenazi (Central and Eastern European) Jewish background.
>
> Regardless, women who have a relative with a harmful *BRCA1* or *BRCA2* mutation and women who appear to be at increased risk of breast and/or ovarian cancer because of their ***family history*** [emphasis added] should consider genetic counseling to learn more about their potential risks and about *BRCA1* and *BRCA2* genetic tests.
>
> **The likelihood of a harmful mutation in *BRCA1* or *BRCA2* is increased with certain familial patterns of cancer** [emphasis added]. These patterns include the following:

For women of Ashkenazi Jewish descent:

- any first-degree relative diagnosed with breast or ovarian cancer; and
- two second-degree relatives on the same side of the family diagnosed with breast or ovarian cancer. "

This form of breast cancer is something not unique to Ashkenazi Jews, as studies have demonstrated that this has also been found in the Hispanic communities in New Mexico and Colorado--who did not know they were descended from Sephardic Jews who had hidden their Jewish identity to survive the Inquisition in the 15th century. This is described in Jon Entine's *Abraham's Children: Race, Identity and the DNA of the Chosen People* , by the Smithsonian in their article, *The Secret Jews of San Luis Valley,* and *The Wandering Gene and the Indian Princess: Race, Religion, and DNA*[8]

People who have had members of their families diagnosed with breast cancer need to know whether past family members may have also died from this disease, in order to determine if it is inherited. Both current and future generations need to have this information in order to make decisions about whether to prophylactically remove both breasts and ovaries (which can mean the difference between early detection and treatment versus possible early death). This is something both men and women need to be able to research--as either can be carrying the gene mutation. The SSDI is a critical tool in assuring researchers that the records they have located on possible ancestors are indeed the correct persons, especially when they have a common name.

We use this as only one example of inherited diseases that require the ability to research ancestry using a SSN—regardless of ethnicity.

Working with Coroners to Identify Deceased's Next of Kin

People are going to their graves with no family to claim them. Medical examiners and coroners' offices—frequently overstretched with burgeoning caseloads—need help in finding next of kin of the deceased. The deceaseds' identities are known; it's their next of kin that are unknown in these cases. Over 400 genealogists are now offering their volunteer services to help locate the next of kin for unclaimed persons. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See unclaimedpersons.org

Working with the Military

There are literally tens of thousands of United States Veterans' remains left unclaimed throughout the Nation. Sometimes decades pass while these remains are waiting to be identified as Veterans and given a proper military burial. Genealogists work with the military to locate relatives of soldiers who are still unaccounted for from past conflicts. By finding relatives, the military can identify soldiers using DNA, and notify the next of kin so the family can make burial decisions. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family [9].

Genealogy as a Profession

While there are millions of people who actively study and research their family history as an avocation, there are many others who earn their livelihoods as professional genealogists. Professional genealogists use the SSDI to (1) help track heirs to estates, (2) find title to real property, (3) find witnesses to wills that need to be proved, (4) work on the repatriation projects [see Working with the Military], (5) track-works of art—including stolen art—and repatriation of looted art work during the Nazi era of World War II, and (6) assist in determining the status of Native American tribes and tribal members to prove–or disprove—that they are entitled to share in Tribal casino revenues.

IRS Needs to Be More Proactive

If the IRS were to routinely run Social Security numbers included in tax returns against the death index, they might avoid giving refunds to deceased individuals.

"Operation Rainmaker" (also known as Operation TurboTax), was a tax fraud operation in the Tampa Bay area. Law enforcement interviews specified that the IRS, while cooperating with other law enforcement officers, is not authorized to share information with local law enforcement departments, hampering efforts to protect their citizens. If the federal government is serious about addressing identity theft that uses a person's Social Security number, then the IRS needs to be given legislative authority to share information with local, county and state law enforcement organizations. It was also stated that filing tax refunds for under $10,000 will not get any attention. As "Operation Rainmaker" found the average tax fraud was about $9,500, below the $10,000 threshold [11]. This is another practice that the Congress needs to review, as the criminals who are perpetrating this fraud know they will be undetected!

It also became apparent in Mr. Agin's case that the IRS assumes the first person filing is the "legitimate" filer and by inference, the second filer is the fraudulent party. The IRS needs to amend their practice when the filing involves a deceased child, to require some verification to determine which is a valid filing.

Unfortunately, since the IRS advocated electronic filing of tax returns, one unexpected consequence is the remarkable increase in tax identity theft.

Support For Efforts to Cease Identity Theft

- If income tax returns were electronically compared to the Master Death File, matching cases could be flagged for special processing, and the person attempting to create a tax fraud could be stopped before the fraud occurs.

- A parent's social security number should be required when filing a tax return for any minor. It is an extremely rare occurrence that a minor child would not be listed as a dependent on the parent or guardian's tax filing. If the minor dies, the IRS could have a procedure to flag any filings without the parent's social security number, again preventing the fraud. Draft legislative language was provided to the Subcommittee staff on January 24, which would facilitate just this prevention of identity theft perpetrated on children. The *National Taxpayer Advocate's Report to Congress for 2011* specifically highlights the benefits of the IRS Issued Identity Protection PINs [10] and suggests that taxpayers should be allowed to turn off their ability to file tax returns electronically. Any family that suffers a death could elect to turn off the electronic filing ability.

- Criminal penalty statutes for those who fraudulently use Social Security Numbers, including, but not restricted to, those who misuse their positions (*e.g.*, hospital, medical institution and office personnel, financial and credit card organizations personnel, prison corrections officer, college or university registrar etc.)

For the reasons stated above:

- genealogists are **NOT** the cause of identity theft;

- genealogists have legitimate, professional and life saving reasons to have immediate access to the SSDI; and

- proactive measures are needed to prevent identity theft and vigorously pursue and punish the **TRUE** identity thieves,

IAJGS respectfully and vehemently encourages the Subcommittee to continue the commercial version of the Death Master File, known as the Social Security Death Index, to be available to the public.

On behalf of the International Association of Jewish Genealogical Societies we appreciate the opportunity to submit our comments, and for the occasion to bring to the Subcommittee's attention the many services the genealogy community performs for local, **state and federal government offices.** We look forward to working with the Subcommittee and staff to find an accommodation that provides genealogists with immediate access to the SSDI.

Respectfully submitted,

Jan Meisels Allen

Jan Meisels Allen
IAJGS Vice President
Chairperson, IAJGS Public Records Access Monitoring Committee

---

1 http://www.identitytheft.info/breaches09.aspx

2 http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer breach/
http://www.nctimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html
http://www.qctimes.com/news/local/article_06d38e24-146a-11df-91c6- 001cc4c03286.html
http://www.washingtonpost.com/politics/tricare-military-beneficiaries-being-informed-of-stolen-personal-data/2011/11/23/gIQAcRNHtN_story.html
http://sundayherald.com/news/heraldnews/display.var.2432225.0.0.php
Copes, H., and Vieraitis, L.M. (2009). Understanding identity theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, *34*(3), 329-349

3 http://consumerist.com/2010/03/id-theft-ring-used-hospital-records-for-300k-shopping-spree.html;
http://articles.sun-sentinel.com/2010-11-11/health/fl-hk-holy-cross-id-20101110_1_identity-theft-ring-patient-files-emergency-room
http://www.miamiherald.com/2011/12/07/2536190/miami-va-hospital-employee-charged.html;

4 http://corporate.ancestry.com/press/press-releases/2012/01/ancestry.com-partners-with-historical-society-of-pennsylvania-to-bring-the-states-rich-history-online/
This survey was conducted online within the United States by Harris Interactive via its QuickQuery omnibus product on behalf of Ancestry.com from August 5-9, 2011 among 2,950 adults ages 18 and older

5 Mayo Clinic staff: "Medical History: Compiling your medical family tree,"
http://www.mayoclinic.com/health/medical-history/HQ01707;

6 https://familyhistory.hhs.gov/fhh-web/home.action

7 http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA

8 Abraham's Children: Race, Identity, and the DNA of the Chosen People. Jon Entine, Grand Central Publishing, New York, N.Y. 2007
http://www.smithsonianmag.com/science-nature/san-luis-valley.html
The Wandering Gene and the Indian Princess: Race, Religion, and DNA. Jeff Wheelwright. WW Norton & Co. New York, NY, 2012.

9 http://www.aarp.org/relationships/genealogy/info-06-2011/genealogy-tips.html
http://www.familiesforforgottenheroes.org/Genealogist.htm

10 http://www.irs.gov/pub/irs-pdf/p2104.pdf

11 http://www.youtube.com/watch?v=gpgTFO7nMBk

MY name: Prof. James W. Brann, former chair of Journalism Department, Boston University.

My address: 260 Eight Rod Way, Tiverton RI 02878 Phone: 401 624-1814. E-mail: jwbscoop@gmail.com.

I was a reporter for many years and worked for The National Commission on the Causes and Prevention of Violence,

established by LBJ. I was co-director of the study on the violence at San Francisco State College. And I have

published articles in The Washington Post, The Chronicle of Higher Education, Columbia Journalism Review,

American Journalism Review, Science Digest, Saturday Review, The Harrisburg Patriot News, The National

Observer, The New Republic, The Providence Journal, The Nation, Commonweal, The Boston Globe, The Boston Herald, and many other

places. I am currently writing a biography of Dr. John Silber, president of Boston University for many years.

And I am an ex-marine.

For many years, I taught journalism students how to use the SSDI. It is an invaluable tool and I strongly urge you to

allow the public continued access to it.

Sincerely,

James W. Brann

emeritus professor of Journalism

Boston University

I am opposed to Congressman Johnson's proposed "Keeping IDs safe act of 2011" (H.R. 3475).

I am a retired city planner and former high school and community college teacher. Now, I am an amateur genealogist, who has been working on my family tree for the past 15 years.

I use the free access to the Social Security Death Index fairly often to validate a family relationship, to get a year and month of death, or to get a hint as to the last place the relative might have lived so that I can look for more information at that location. Typically, I do not need to send for a copy of the application, and I rarely need to use an actual social security number to narrow down a family member. But, I should have a right to see it for purposes of record keeping.

The proposed act will NOT keep IDs safe. It will merely restrict public information and make it much more difficult for researchers, whether private or academic, to gather information that should be publicly available.

Social security numbers are available all over --especially those of the folks dying now . These numbers come from old work or school records, old credit and mortgage applications, old medical records, old military or passport applications, as well as numerous other sources currently in the public records that might have included the numbers as a tracking mechanism.

Even if the numbers were further restricted, the proposed law would fail to protect ID as intended. The law would just makes it much more difficult and costly for an average person to obtain information about a family member or historical figure that he or she has a right to see. What is happening to the freedom of information rights that we used to have?

I see the proposed law as just another attempt at censorship in a free society.

The numbers are easily obtained by internet hackers, mail thieves and even dumpster divers. If there is a will to do harm, such as stealing identities, the creative criminal will figure out a way to do it. Once you start restricting information (other than that what is clearly for national security purposes) where do you stop?

Please kill this bill that would further restrict our rights to information in a free society.

Dear Honorable Congressmen and Congresswomen,

I have to admit that I, like so many other Americans did not know who to write to when faced with a devastating realization of a tragic misuse of government provided information. A quick search online brought me to you. Let me share with you what is literally ripping my heart out right now.

On September 08, 2011 my 17 year old son Joshua Miller was killed in a car accident when he fell asleep at the wheel, crossed the center line, and collided head on with an oncoming truck. His death has tested the limits of our family's endurance as we strive to continue with a new kind of normal that has enveloped our lives. For the record, he was wearing his seat belt, he was not using his phone as it was found in his pocket, he was a good boy that attended church three times a week and was working hard to save enough money to buy some land where he could eventually become his dream, a farmer.

On January 25th, 2012 I did what so many Americans do this time of year; I attempted to file our taxes online. The return was rejected because someone had already filed using one of the dependent social security numbers on my return. I contacted the IRS and was told that there was nothing I could do to resolve this except to file our return by paper and wait six weeks to twelve weeks for a response. They also would not tell me who had used one of my children's SSNs nor could they even tell me which one had been used. I expressed to the agent on the phone how horrible and sick I was feeling and that I suspected it was my son's SSN that had been violated in this way. Because of privacy concerns though, she could not disclose to me even the identity of my own child. She did however, probably against policy, recommend that I could use a process of elimination by removing my children one at a time from our tax return and trying to submit it again to see if it would be rejected. I did so and quickly found out that my suspicions were correct; it was my son whose SSN had been stolen. Out of fairness, the agent did tell me that it could have been a typo but this is hard to believe as the records are verified against the name submitted and must match or it will generate a different rejection error. The hardest part is that we are now left with the burden of proof and must submit documentation in writing to correct this situation. There is no information that will be shared with us, no knowledge as to if someone will be prosecuted for this terrible violation of our grieving process. This has re-opened wounds that run very deep and have left us having to fight to prove that the son we love beyond measure, the son that is now absent from his body and prayerfully present with the lord, our precious baby boy, is so much more than a money making opportunity for some lowlife con-artist. We have been robbed of our right to be left in peace to deal with the loss of our son. Who is to blame for this?

As it turns out, you are if you do nothing to change the laws as they are currently written. A quick search on the internet will show you that this happens all the time. Deceased children are an easy target for would be thieves because upon the death of anyone in this country the private records of the deceased immediately become very public. This includes the social security number as well as all other identifying information that a would-be-thief would need in order to steal a deceased person's identity. All an identity thief has to do is watch for death notices of any child that would be of value to them and then make a public records request to retrieve the information that will allow them to steal a dead child's identity. Once the information is in the hands of the criminal it becomes a race for them to file a fraudulent tax return before the parents are able to file their own valid one. If they file first, the parents are the ones that have to prove they are the rightful party to claim the child as a dependent.

Who will be the voice for my son? I can only write to anyone that will listen and beg them to take up this cause. Why would the social security number of a deceased person ever need to be public knowledge? Why can a parent not register with the IRS or Social Security Administration to not allow the disclosure of this private information? This has opened a chasm of realization that I rather naively assumed that once the record had been flagged as deceased with the Social Security Administration, which it had, that it would become flagged across all government agencies.

So now I will await a response from you. As an elected member of the Congress of our United States, what say you? What explanation can you give to me as to how our government actually fosters an environment where the criminal is right until someone comes along that says they are wrong? My child is being abused from the grave, and our government provided the information that is permitting it to occur. This is not ok.

Respectfully,

Jason Miller
37880 Pleasant Hill Road
Latham MO , 65050
660-458-6594
Citizen

Jay & Deborah Fuller

1251 Muriel Street

Woodstock, IL 60098

815-338-2416

jdandhope@sbcglobal.net

The House Subcommittee on Social Security held the hearing on the pending legislation H.R. 3475.

Please see above for the information from my husband and I regarding who the following comments should be attributed to.

On March 10, 2010 our daughter, age 12, Hope died from a pediatric brain tumor. Upon filing our federal return in January of 2011 for the year 2010 we were rejected due to a problem with our daughter's (our deceased daughter's) social security number. If the tragic loss of our daughter wasn't enough a thief had stolen her identity. Please help protect our families by supporting the pending legislation H.R. 3475. It is my understanding that those in the genealogical world feel they have a right to all our kids' information. That cannot possibly be fair to us or our dead children.

Thank you

Jay & Deborah Fuller

(Parents of Hope Alizah Kimlee Fuller 6/26/97-3/10/10)

February 16th, 2012

To: Committee on Ways and Means

From: Jay Johnson, mother of a deceased 5 year old DIPG Child
2869 Lansford Ave. San Jose, California 95125
408-655-2817
email: jayrjohnson#@yahoo.com
Hearing: HR 3475

There are many cruel things that come with pediatric cancer. There are hours of treatment, which includes radiation and chemotherapy. Watching your child bravely deal with those treatments and their cruel side effects is heartbreaking. There are the missed hours at school, hours a child should be playing and being with their friends. There is the cruelty of a child suffering the effects of brain tumor, specifically this one, such as loss of motor abilities while retaining a sharp cognition. When your child dies, there is the heartache and despair of lost dreams, hopes, and innocence. There are many financial burdens that pediatric cancer parents endure. All of these we have no control over.

But, the identity theft brought on after your child dies is a very low blow. Our family did what it thought was best to protect ourselves. Our son passed away June 5, 2011. We quickly filed our 2011 tax returns as soon as humanly possible, February 6, 2012. That did not seem to matter, someone has already claimed our son as their dependent. What else can we expect? His name, birthdate, social security number is fully available on the Death Master List. Anyone can access that information and for FREE. In addition to the IRS, we are now contacting all the credit agencies to ensure there is nothing else stolen under his name. I don't understand the need to publish FULL social security numbers of our deceased children. I would be fired from my job at eBay if I even accidently disclosed a single social security number. What has happened to data privacy protection in this country! The fact that is okay for the genealogical companies' to publish this information for anyone to see is mind numbing to me.

Please stop the publication of FULL social security information of the Death Master List. And, to the fullest extent permissible, please prosecute the scum that fraudulently claim these children as dependents when filing tax returns.

Sincerely,
Jay Johnson, father to this precious deceased boy

Name: Jerry Sherard
Address:
429 S Moore St.
Lakewood, CO 80226-2629
Phone: 303-988-9530
email: shep964ard@hotmail.com
Hearing Title: Social Security Death Records

H.R. 2475 Keeping IDs Safe Act of 2011

As a genealogist, I have found the SSDI to be a very valuable database in helping people find out information about their deceased ancestors.

The SSN is required to access many records of genealogical value:

United Mine Workers of American pension records.
Railroad Retirement Board pension records.
Recent military records (I know my military service number is my social security number).
The SSDI provides a death date for finding obituaries and death certificates.
The SSN narrows the search for finding a death date or death certificate for common names, for example for John Smith.

I am opposed to the passage of H.R. 2475 which covers Social Security Death Records.

My name is Joette Kunse, 9740 Reese Rd., Clarkston, MI 48348, phone 248 620 2984, email jkhorses@comcast.net Oakland County Genealogical Society

I'd like to submit a statement for the Death Records Hearing. As a family genealogist and a workshop leader in genealogy, the Social Security Death Index has been a valuable tool in pursing relatives who have passed on. While I understand the issues with fraud, I would assume with technology, there could be blocks on particular numbers. The SSDI is a valuable tool for genealogist and one of the only tools to find relatives who have passed on in the 20th century. People have moved from their hometowns starting around WWI and the SSDI which begins in 1932 helps tremendously in searching for relatives. Sometimes you need to find a technology work around versus just closing down the SSDI to the public.

I would hope that you would take my thoughts into consideration as you did not allow representatives from the National Genealogical Society to speak. Why would you ignore a portion of the population.

Joette Kunse

Please take action to prevent the DMF from being released to the public. I know many families who have lost children to cancer – only to find that their child's identity has been stolen for tax fraud purposes. This is so painful for the family to resolve. You can take action to prevent this pain in the future. Please do so. Ease of access for a hobbyist (such as genealogy researchers) does not trump the obligation we have to American families who have lost their child. Thank you.

John Mackintosh
12 Highland Meadow Dr.
North Attleboro, MA 02760
(508) 399-8814

John.j.mackintosh@gmail.com

Comments on **Chairman Johnson Announces a Hearing on Social Security's Death Records**

Eliminating this important data would have a lot of detrimental effects in my opinion.

While I do not use this data daily it was quite important for me personally in trying to find out where and when my grandfather passed away. He had simply left town many years previously and without this resource we would have had no clue if he was alive or not. Because of this data we found out not only when he passed but where.

Another positive use of the death information is to prevent a grieving spouse or family member from receiving unwanted correspondence. Many companies and non profits alike do not want to mail or correspond with a deceased person. The costs to businesses and non profits alike would be high and get higher each and every year. The feelings of the deceased spouse receiving the continued reminder that a loved one has passed also need to be considered. Mail is only going to get more expensive as well. Most of the recently deceased are by and large not as technically literate as the younger generation so mail is still the overwhelming choice of seniors.

Folks like my sister enjoy doing family research and doing family trees and there are a lot of them who use this data, so this would also negatively harm all these folks who enjoy this pastime.

I cannot condone identity theft certainly and applaud efforts to stop it. This bill would hurt a lot of legitimate and honest uses of the data because of the actions of a few. There must be some alternatives technically speaking and I cannot help but feel our technical gurus could figure out something in lieu of this rather draconian approach. Thanks for your consideration.

John Wright

1689 Anne Court Annapolis, Maryland 21401

410-849-2143

Jhwright14@verizon.net

Social Security Administration's Death Master File

I just want to say that the simple suggestion that the release of the SSDI will be blocked has already made my genealogical research more difficult. My research is difficult enough because my mother has been married 5 times and my husband was adopted. The worst thing that can happen is to have more legitimate family records blocked from my view. Real research, in any field, cannot be based on rumor and innuendo so please do not take any access to vital records/documents away from family historians. Every individual has a right to know the truth about their origins from real documents not just from family lore.

Judy Darnell, personal genealogist
Newsletter editor for St. Clair County Genealogical Society (St. Clair Co., IL)
7329 MacLeod Lane
Dardenne Prairie, MO 63368
636-281-9810
Judydarnell@charter.net

While the Death Master File may provide information that can be misused, it is not reasonable to deny the information it contains to legitimate requestors. Terminating all access is akin to saying that because some teenager has huffed (inhaled with the intent to get high) spray paint, I may not purchase some Rustoleum to touch up my barbeque grill, even though a) I have a legitimate use, and b) I'm 57 years of age.

Reasons to find ways to prevent abuse rather than terminate all access include:

- The information contained in the Death Master File is crucial to genealogical searches by individuals interested in tracking down their ancestors.
- The information being misused is not the fault of the Social Security Administration, but rather that of malicious third parties.
- Eliminating access to the Death Master File will not eliminate identity theft; accessing state and local death records by those intent on malfeasance won't be impacted by restricting or eliminating access to the Death Master File. Information on how to obtain fake identities is readily available in books and online.
- Erroneous reports of individuals' deaths can be resolved by tasking SSA personnel with double-checking provided information; this prevents malicious as well as accidental erroneous reports. Failing to check information is probably the biggest flaw in the system by far.

The information in the Master Death Record should be able to be accessed by the public through legitimate genealogical and governmental agencies and restricted to those with legitimate reason for accessing the information. If someone is later am found to have misused that information, fine them or refuse further access, but don't penalize everyone for the actions of a few bad actors. Abuse of the data doesn't justify total access elimination; after all, people write in library books, fail to return them, or accrue excessive book fines without libraries being shut down en masse due to 'abuse'.

Thank you for taking my comments into consideration in your deliberations.

Karen Isaacson
Woodinville, WA 98077-7808

Kathleen S. Johnson

602 9th Street

Scribner, Nebraska 68057

Phone: 1-402-664-3256

E-mail: ksjscrib_city@yahoo.com

The Ways and Means Committee

Hearing on Social Security's Death Records – 2 Feb 2012

28 Jan 2012

Dear Chairman Johnson,

I am writing in regard to the Social Security Death Records and the current discussion in your committee about the Death Master Files. I am a tax paying citizen and an amateur genealogist. I use the Social Security Death Master Files on a daily basis, to verify the death dates of the people that are my relatives. The actual Social Security number, that is also recorded with the files are not as important to me as the full name, address and birth and death date that are recorded. It is imperative to have the correct death date to continue with my work in search of supporting documentation. Closing the files to the general public would be very detrimental to my work. I encourage your committee to continue to keep the Death Master files available to the public for the legal use of tax paying citizens in genealogical research.

Thank you for this opportunity,

Kathleen S. Johnson

U.S. Citizen

January 30, 2012

Representative Sam Johnson (R-TX)
U.S. House of Representatives
1211 Longworth Building
Washington, D.C. 20515
202-225-4201

Re: HR 3475, to prevent public access to SSDI; Keeping IDs Safe Act of 2011

Senator Bill Nelson
U.S. Senate
716 Hart Senate Office Building
Washington, DC 20510
202-224-5274

Re: SB 1534, to prevent disclosure of deceased's social security number for two years.

Gentlemen:

As you know, Congressman Sam Johnson, Chairman of the House Committee on Ways and Means Subcommittee on Social Security, has organized for the Subcommittee to hold a hearing on the accuracy and uses of the Social Security Administration's Death Master File, with commercial name Social Security Death Index (SSDI), on Thursday, February 2, 2012 in B-318 Rayburn House Office Building, starting at 9 am.

Because of problems where a few living people are mistakenly identified as deceased and where, rarely, social security numbers of dead children are stolen by thieves who use the stolen numbers on IRS returns to claim tax benefits, Congress is reacting wildly, by proposing to shut down all public access to SSDI. I suggest you review the specific draft comments dated January 24, 2012 to Rep. Margaret Hostetler on the House Ways and Means Committee, by Jan Meisels Allen, Managing Member, Records Preservation and Access Committee, c/o Federation of Genealogical Societies, PO Box 200940, Austin TX 78720-0940, with phone 1-888-FGS-1500 and any follow-up comments.

I would like to say generally, that as a volunteer genealogist, who works occasionally as a volunteer with my local DAR chapter and occasionally, for free, with distant relatives and friends, to trace family histories, that we find the SSDI useful. When one has general information for a deceased relative; such as name, range of two to three states, and a five-year range for death; one may find confirming information with SSDI, such that one then may contact the town library and ask for newspaper obituaries or death notices. One then may learn the cemetery where the deceased person is buried and, sometimes, next of kin.

Public access to SSDI is important. Please don't "throw the baby out with the bathwater," by imposing onerous conditions on public access to SSDI.

Thank you for your attention.

Sincerely,

Kathryn E. George (MD District 8, that is being redistricted)
16625 Alden Av
Gaithersburg MD 20877-1503
301-869-4948
kay.george@verizon.net

copies:
Rep. Chris Van Hollen
Capitol Hill Office
1707 Longworth H.O.B.
Washington, DC 20515
202-225-5341

Rep. Roscoe Bartlett
Capitol Hill Office
Rayburn House Office Building
Washington, D.C. 20515-2006
202-225-2721

Senator Barbara Mikulski
503 Hart Senate Office Building
Washington DC 20510
202-224-4654

Senator Ben Cardin
509 Hart Senate Office Building
Washington DC 20510
202-224-4524

January 30, 2012

Keith B. Riggle
304 Briar Ln
Morris IL 60450

Chairman Sam Johnson
United States House of Representatives
House Ways and Means Committee
Subcommittee on Social Security
Washington, D.C. 20515

Subject: Hearing on Social Security's Death Records

Dear Chairman Johnson:

I would like to tell you how I, as a genealogist and family historian, use the Social Security Administration's Death Master File (aka Social Security Death Index [SSDI]).

I use the SSDI to appropriately identify records of people when tracing my family history, especially if the person has a common name. The SSDI is especially helpful in constructing family medical histories. There are several inheritable diseases in my family, including diabetes and Parkinson's disease. Genealogy assists in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The Social Security Number is critical to make certain that I have the correct person. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family (1). Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative (2).

I support Congress's intent to protect Americans from improper usage of their personal information and to protect them from identity theft. However, denying the millions of Americans who engage in genealogy access to the SSDI is not the answer. Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and

corporate databases was [sic] either lost or stolen" (3). The SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (http://tinyurl.com/yb6e49e), it states that the Death Master File (SSDI) prevents identity fraud, as it verifies a person's death. In addition to family history researchers, the SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others. The IRS should use the SSDI to identify fraudulent tax returns.

The Records Preservation and Access Committee of the Federation of Genealogical Societies, National Genealogical Society, and International Association of Jewish Genealogical Societies has presented you with a position paper on this subject. As an individual genealogist, I fully support their position and recommendations.

Keith B. Riggle

---

(1) Mayo Clinic staff: "Medical History: Compiling your medical family tree," http://www.mayoclinic.com/health/medical-history/HQ01707
(2) https://familyhistory.hhs.gov/fhh-web/home.action
(3) http://www.identitytheft.info/breaches09.aspx

KENNETH H. RYESKY, ESQ., STATEMENT FOR THE RECORD, HOUSE COMMITTEE ON WAYS AND MEANS, SUBCOMMITTEE ON SOCIAL SECURITY, WRITTEN COMMENTS ON PROVISIONS RELATING TO SOCIAL SECURITY ADMINISTRATION'S DEATH MASTER FILE.

I. INTRODUCTION:

House Committee on Ways and Means Subcommittee on Social Security held a Hearing on 2 February 2012, regarding the accuracy and uses of the Social Security Administration's Death Master File. Public comments were solicited. This Commentary is accordingly submitted.

II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:

Background: The Commentator, Kenneth H. Ryesky, Esq., is a member of the Bars of New York, New Jersey and Pennsylvania, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York, where he teaches Business Law courses and Taxation courses. Prior to entering into the private practice of law, Mr. Ryesky served as an Attorney with the Internal Revenue Service ("IRS"), Manhattan District. In addition to his law degree, Mr. Ryesky holds BBA and MBA degrees in Management, and a MLS degree. He has authored several scholarly articles and commentaries on taxation, including one made part of the printed record of a hearing before the Senate Finance Committee. [1]

Mr. Ryesky also engages in genealogical research, and has thereby facilitated the reconnection of relations within his own family approximately six decades following the cut-off of communications with siblings in the old country which was imposed upon his grandfather by the repressive policies of the Soviet Union.

Contact information: Kenneth H. Ryesky, Esq., Department of Accounting & Information Systems, 215 Powdermaker Hall, Queens College CUNY, 65-30 Kissena Boulevard, Flushing, NY 11367. Telephone 718/997-5070 (vox), 718/997-5079 (fax). E-mail: khresq@sprintmail.com.

---

[1] *Tax: Fundamentals in Advance of Reform*, Hearing before the Committee on Finance, U.S. Senate, 110th Congress, 2nd Session, April 15, 2008, S. Hrg. 110–1037, pp. 113 - 150 <http://finance.senate.gov/library/hearings/download/?id=fead52be-a791-4105-96da-0010264cd7ed>.

Disclaimer: Notwithstanding various consultations between the Commentator and other interested individuals and organizations, this Commentary reflects the Commentator's personal views, is not written or submitted on behalf of any other person or entity, and does not necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

III. COMMENTARY ON THE ISSUES:

A. Overview:

The Social Security Administration's Death Master File (DMF) [2] is a publicly-available resource of great value to several constituencies, including but not limited to genealogical researchers. But information from the DMF has also been used by unscrupulous individuals for nefarious purposes, including tax fraud. The imperatives of genealogical research and sound tax administration are now on a collision course; nay, they have already collided. Congress now seeks to address the issues regarding the DMF, including H.R. 3215, H.R. 3475, H.R. 3482, S.1534, and including the subject Hearing.

The Commentator now provides to the Subcommittee his perspective, from his personal and professional backgrounds in both tax administration and genealogic research, on the intersection between those two areas.

B. Genealogical Research:

In addition to those who engage in genealogical research as gainful employment, there are many, many more, the Commentator included, who do it in other contexts. The Commentator is very disinclined to refer to these other individuals as "amateurs" or "amateur genealogists" because their research all too frequently is no less extensive, informative, scholarly or successful than that done by the professionals who research genealogy for a living. Accordingly, this commentary will use the term "individual researcher" and similar terms to refer to such persons.

---

[2] The DMF is available and utilized in another incarnation known as the Social Security Death Index (SSDI), and is often referred to as such.

Genealogical research plays a vital role in diverse areas of law and society. These include, but are not limited to, identifying the heirs to a decedent's estate, [3] and in such a context, an attorney using the skills of an individual researcher can perform the required diligent search for heirs without burdening the decedent's estate with the expense of a professional genealogist. [4] Indeed, the Commentator has had occasion, in a probate proceeding, to use his individual genealogical research skills to locate heirs theretofore unknown and/or believed deceased by the friends of the testator.

Genealogical research can determine title to real property, [5] and qualification for loan guarantees for housing. [6] Genealogical research is often vital to determining the status of Native American tribes and tribal members [7] (and in such regard, figures into the legal battle over competition against retailers of tobacco products from the untaxed tobacco products sold by Indian tribe members). [8]

The effective repatriation to Americans and others of artwork looted during the Nazi era requires genealogical research data. [9]

---

[3] *In re Estate of Wright*, 1997 Del. Ch. LEXIS 26 (Del. Ch., 1997); *Matter of Swingearn*, 2011 N.Y. Misc. LEXIS 6019, 2011 NY Slip Op 33230(U) (Surr. Ct., Nassau Co., 2011); *In re Estate of Rosen*, 819 A.2d 585 (Pa.Super 2003).

[4] *See, e.g., Matter of Marsden*, 2009 N.Y. Misc. LEXIS 6347 at *7, 2009 NY Slip Op 33235(U) at *5 (Surr.Ct., Nassau Co., 2009).

[5] *Eaton v. Town of Wells*, 760 A.2d 232 (Me. 2000).

[6] 12 U.S.C. § 1715z-13b(a)(6)(B)(i); 24 C.F.R. § 1007.5.

[7] *James v. Dept. of Health and Human Services*, 824 F.2d 1132, 1138 (D.C.App. 1987); *Muwekma Ohlone Tribe v. Salazar* , 2011 U.S. Dist. LEXIS 110400 at *15 - *16 (Dist. D.C. 2011); *Timbisha Shoshone Tribe v. Dept. of Interior*, 2011 U.S. Dist. LEXIS 51892 at *2 - *3 (E.D. Calif. 2011); Kirsty Gover, *Genealogy as Continuity: Explaining the Growing Tribal Preference for Descent Rules in Membership Governance in the United States*. 33 AM INDIAN L REV 243 (2008/2009).

[8] *See Gristede's Foods, Inc. v. Unkechauge Nation*, 660 F. Supp. 2d 442, 447 - 448 (E.D.N.Y. 2009).

[9] Statement of Catherine A. Lillie, p. p. 26, Review of the Repatriation of Holocaust Art Assets in the United States, Hearing Before the Subcommittee on Domestic & International Monetary Policy, Trade, &Technology, Committee on Financial Services, U.S. House Of Representatives, 109th Cong., 2d Sess., Serial No. 109–113, at p. 26 (27 July 2006) <http://archives.financialservices.house.gov/pdf/ArchiveHearing/109-113.PDF>.

And fees paid by genealogical researchers are a source of revenue for the United States government. [10]

Genealogical research, then, is a serious and salient matter which cannot be viewed merely as some sort of quaint pastime. Opportunities for individual researchers need to be fostered and facilitated, with due regard for the role it plays in so many areas and aspects of law and society.

There are, of course, limitations to the diversity of witnesses who can be called to any given Congressional hearing. Standing alone, the failure of the Subcommittee to invite testimony from the genealogical community (both the professionals and the individual researchers) denied a significant number of legitimate stakeholders of an opportunity to give their vital input. The Subcommittee now needs to pay serious regard to the materials in addition to this instant Commentary that surely will be submitted from members of the genealogical community, whether from professional genealogists, individual researchers, or the genealogical interest groups and societies.

C. Social Security Numbers and Tax Administration:

This Commentator has previously expounded, at greater length, to a different Subcommittee of the Ways and Means Committee, on the American system of voluntary compliance with the tax laws. [11] It now suffices to state that the American voluntary compliance system is a far less repressive alternative to other systems elsewhere, currently and in bygone days, but that the uncoerced compliance so vital to the system depends, in no small measure, upon the security of taxpayers' personal data.

In the taxation context, data security means more than restrictions on access to the data. Data security also refers to how data is processed. The failure to correctly process or verify data poses security issues no less deleterious than the improper access to that data.

---

[10] *See* 8 U.S.C. § 1356(t); 8 C.F.R. § 103.7(b)(1)(i) (E) & (F).

[11] Statement of Kenneth H. Ryesky, Esq., *Hearing to Examine Tax Fraud Committed by Prison Inmates*: Hearing before the Subcommittee on Oversight of the Committee on Ways and Means, U.S. House of Representatives, 109th Congress, 1st Session, June 29, 2005, Serial No. 109-36, pp. 62 - 66.
<http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg24905/pdf/CHRG-109hhrg24905.pdf>.

Mr. Agin's testimony at the subject 2 February 2012 Hearing, together with the testimony of Mr. McClung at a recent Senate Finance Committee hearing, spotlight such improper processing of tax information by the Internal Revenue Service. [12] As related by Mr. McClung, his income tax return was rejected because his deceased *dependent child* had already been claimed on a filed return. It is noted that the Social Security Administration's Form SS-5, Application for a Social Security Card, emphatically requires, in the case of an infant child, the parents' Social Security Numbers. In the case of Mr. McClung, the fraudster who claimed his deceased daughter apparently filed a tax return where the person purportedly claiming the McClung infant used a Social Security Number other than Mr. McClung's or his wife's. The failure of the IRS to "red flag" the first return, filed by the fraudster, for further inquiry is a processing failure.

The case of Mr. Agin is similar, but is all the more egregious because Mr. Agin and his wife presumably filed prior tax returns in prior years with their correct Social Security Numbers; the subsequent claiming of the same infant dependent by another purported taxpayer with a different Social Security Number should have been an additional "red flag" for the IRS. And, as further reflected in Mr. Agin's testimony, his case was far from unique.

D. Approaches to Resolving the Conflict:

There are several approaches which Congress ought to take in resolving the conflict between the need to facilitate genealogical research and the need to prevent and punish tax fraud. These might include the following:

1. Criminal penalty statutes for those who fraudulently use Social Security Numbers. These can include criminal sanctions against those who misuse their positions (*e.g.*, hospital records administrator, prison corrections officer, college or university registrar, et cetera).

2. Private causes of action, in the Federal courts and elsewhere, for victims of the fraudulent misuse of Social Security Numbers. This can include statutory damages in addition to actual damages.

---

[12] Statement of Terry D. McClung, Jr., The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth (25 May 2011). <http://finance.senate.gov/imo/media/doc/Testimony%20of%20Terry%20McClung.pdf>.

3. Mandates that the IRS use various data processing parameters and standards in handling, checking and verifying the tax returns it receives from taxpayers. [13]

There seems to be an intent on the part of some members of Congress to restrict the availability of information in the DMF. While some restrictions may well be appropriate, it must be remembered that the DMF is a valuable information resource developed at the expense of the American people, and should be availed to the public for legitimate purposes. The unnecessary restriction of access to the DMF to individual genealogical researchers would not only work an injustice to the American people, but would impede the accomplishment of many legitimate legal and social processes, and would further facilitate the IRS's laxity in its processing of taxpayer information.

E. Conclusion:

The United States Congress has already declared it to be in the national interest to preserve and protect America's historical roots abroad. [14] This being so, it is all the more in the national interest to protect and preserve genealogical information in America. The problem of tax fraud using Social Security Numbers is a significant problem that requires Congressional attention. Resolution of the problem must give not unduly burden the conduct of legitimate genealogical research.

5 February 2012
Respectfully submitted,

Kenneth H. Ryesky, Esq.

---

[13] The IRS has demonstrated broad ineptitude in its tracking and processing of Social Security Numbers *see, e.g. United States. v. Nielsen*, 1 F.3d 855, 857 (9th Cir. 1993), *cert. denied*, 525 U.S. 827 (1998); *Wallin v. Commissioner*, 744 F.2d 674, 677 (9th Cir. 1984); United States v. Shafer, 1996 U.S. Dist. LEXIS 56165 (E.D. Pa. 1996); *Grimland v. Commissioner*, T.C. Memo 1993-367; *In re Washington*, 172 B.R. 415, 418 - 419 (Bankr. S.D. Ga. 1994).

[14] 16 U.S.C. § 469j (establishing the Commission for the Preservation of America's Heritage Abroad).

Dear Sirs and Madams,
I am an heir locator and use the online SSDI daily in my efforts to find heirs and inform them of their entitlement to Estates in the U. S.

Over the last 14 years I have been able to locate dozens of heirs in the U. S. and abroad and as a result they have received a total of several million dollars.

It would be cumbersome to detail the process but in most cases it begins with a search on the SSDI. This then leads to other helpful information and, in the case of intestate succession, creating a family chart and contacting next-of-kin.

It is only just that family members be informed of the death of their relative and the financial boon to them. In my experience, it has changed the life of a child with Down's Syndrome and a mother with a child battling cancer. These are just two examples.

It seems we are too preoccupied with privacy at the cost of our fundamental values of justice, fairness, family rights and property rights. There must be a better way to prevent criminals and terrorists from achieving their ends without sacrificing our values and harming the innocent.

Please vote to continue to allow online public access to the SSDI.

Sincerely,
Laura Peritore
lpclaims@pacbell.net

To: waysandmeans.submissions@mail.house.gov

Leslie Brinkley Lawson
5180 SW 198th Ave
Aloha, OR 97007-2964
503-649-6679
Leslie@LawsonResearch.net
Social Security Death Records

As an American Citizen I am writing in regards to the following bills before the committee:

• HR 3475, Keeping IDs Safe Act of 2011 http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
• S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9 (If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
• HR 3482 To prevent identity theft and tax crimes.http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
• HR 3215 To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

First, I must say how incensed I am as an American citizen that I have been shut out of the process regarding the closer of SSDI. By refusing to allow genealogists to testify and convey to you how important this record group you have sent a strong message to this individual voter. This decision affects my business greatly; the loss would affect me in an insurmountable way. I am a forensic genealogist. My job is to recreate family groups from very broken families to find heirs to estates or to figure out who their family is when they are no longer able to speak for themselves (dementia, Alzheimer's, brain injury). If you remove access to the SSDI you cripple the identity process used by forensic researchers. I ask that you reconsider these actions by reviewing the information noted below.

It has been proven time and again that identity theft has nothing to do with the SSDI, and everything to do with computer hackers. Please refer to the 2009 Security Breaches and Database Breaches.

It might be better to require business to use the SSDI to prove they aren't hiring someone who is fraudulently using the number of a dead person. Require credit card companies to use the SSDI before approving credit cards for every person they extend credit to.

• Genealogy is a serious profession.

• Genealogists use the SSNs to appropriately identify records of people when tracing family medical history, especially if the person has a common name: Sara Cohen, Tom Brown, Jose Martinez, Trung Lee, etc. Genealogy assists in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The SSN is critical to make certain that one has the correct person. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family. Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative.

• Genealogists work with coroners to find next of kin for the deceased. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See unclaimedpersons.org

• Genealogists work with military to locate relatives of soldiers who are still unaccounted for from past conflicts. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family.

• Other stakeholders who are concerned and want full and immediate access to the SSDI include: the financial and insurance industries [they need the information timely so that they can verify deaths to pay out death claims and verify beneficiaries for paying retiree benefits]; federal, state and local law enforcement agencies; Lexis-Nexis; charities legacy departments and planned gifts departments, medical researchers [tracking morbidity cluster deaths and tracking mortality of medical trial results]; state, county government and teacher retirement funds; county assessment offices, student loan companies; universities for student loans, tracing alumni mortalities and other activities, enhanced collections department of state courts, and other stakeholders that we are learning about daily.

We need this database left whole. Its benefits far outweigh the negative press.

Thank you.

Leslie Brinkley Lawson
Forensic Genealogist
http://www.lawsonresearch.net/

Linda M. Dodge
9 Hastings St.
Stow, MA 01775
lrldodge@aol.com

Dear Ladies and Gentlemen:

As an amateur genealogist for many decades, I appeal to you. Please do not limit our access to the social security records of people who have died. This is an invaluable source for those of us who seek to locate our ancestors and find out where we come from.

Thank you.
Yours truly,
Linda Dodge

1 February 2012

Re: Hearing on Social Security Death Master File

Thank you for the opportunity to provide input to the discussion about the accessibility of the Social Security Death Master File (SSDI). I am a professional genealogist and also do family history research for my own family. I have used the Social Security Death Index on CD-ROM and the Internet for nearly 20 years. It is extremely valuable for tracking family migrations and identifying what happened to people after they "disappear" from the family. The Social Security Death Index is often the only key that can open up doors to additional publically available information, such as obituaries and death records, when applicable.

I ask that you do not restrict public access to the SSDI. American families are relying on it to help discover and reconstruct their family histories.

Also, I know that organizations such as universities and churches use it to update their alumni and membership lists when members move away and the organization is not informed of their death. And heirship attorneys use the SSDI to help track down potential heirs to estates.

The value of keeping the SSDI a public record is immense and it must be preserved.

Linda Masden Vixie

3445 Possum Ct.

Colorado Springs, CO 80918

(719) 528-6847

lvixie@comcast.net

February 2, 2012

Committee on Ways and Means
U.S. Congressman Sam Johnson
Chairman Subcommittee on Social Security

Re: Social Security Administration's Death Master File

The La Porte County Indiana Genealogical Society shares the objective of protecting Americans against fraud and of addressing deficiencies in the current operation of the Death Master File. We hope that measures can be developed which address these concerns while preserving to the maximum extent practicable access for genealogical and other legitimate purposes. We urge legislators who work to address these concerns to target the criminal behavior rather than seeking a quick solution whose only real impact is felt by law-abiding citizens, law-abiding citizens who use the index for the myriad of legitimate purposes for which it was created.

Members of our society, the La Porte County Indiana Genealogical Society, have expressed this concern. Through the availability of SSDI, one of our members was led to an uncle he had only met once in person. The uncle was the oldest brother of our member's father who left for California in the 1930's. Only through SSDI, accessed on "Family Search", was the member able to find where and when his uncle died.

Another member, whose father's siblings were tragically separated while they were young children, was able, upon her father's death, to find and communicate the news to numerous cousins whom she had never met. She found several of her deceased aunts and uncles in the SSDI that pointed her in the right direction to find their families.

A third member was searching for her mother's cousin who had not been heard from in many years. For her, a search on the SSDI showed he had passed away and when and where. With this information she was able to contact a newspaper in the area and obtain an obituary to determine the details and any living survivors.

These are priceless experiences, only available through the free and open access to this public information.

The interests of our society and the genealogical community are not hard to understand. Access to records or the lack thereof, is the pivotal issue for us. Without documentation, our family histories are more legend than history. Our society' goals, to collect, preserve and disseminate knowledge and information with reference to genealogy and history, can only be achieved through unfettered access to public records.

We urge that your committee propose ways to target the criminal and not those who serve the legitimate good of the community.

Respectfully submitted,

La Porte County Indiana Genealogical Society
904 Indiana Ave.
La Porte, IN 46350

Alan H. Zeller, President
219-324-0404
alan_zeller@frontier.com

Lester J. Chadwick, Vice President
Harold Henderson, Secretary
Dorothy J. Palmer, Treasurer
Fern Eddy Schultz, Genealogist-Historian

SUPPLEMENTAL SUBMISSION SHEET

LA PORTE COUNTY INDIANA GENEALOGICAL SOCIETY
904 Indiana Ave.
La Porte, IN 46350

Alan H. Zeller, President
219-324-0404
alan_zeller@frontier.com

Marilyn G Hamill
151 Gold Ave NW
Grand Rapids, MI 49504
maggiesten@aol.com
616-454-7515

28 January 2012

RE: **Chairman Johnson Announces a Hearing on Social Security's Death Records, HR 3475**
Thursday, February 02, 2012

Dear Members of the Ways and Means Committee:

The Master Death File aka Social Security Death Index is used by many people and businesses to stop identity theft. It is used to help with repatriation projects to reunite the remains of POW'S with their families; it is used to stop credit card fraud; it is used to stop welfare fraud; it is used to stop tax fraud; it is used in probate cases to determine legal heirs; it is used by the health care industry to track people who have been involved with medical studies; it is used to determine oil and mineral rights; it is used by the organization Families For Forgotten Heroes to find the families of the unclaimed remains of our nation's veterans that are sitting in storage at funeral homes; it is used by the organization Unclaimed Persons to help coroners and medical examiners find the next of kin of people who have passed away.

The SSDI is a very valuable tool that is used by many people who do good works in our country. Please work to protect my right under the Freedom of Information act to access the SSDI. Taking that right away will not fix the problem of identity theft: it will do the opposite and make it easier for criminals to commit that crime.

Thank you for ensuring that my access to this valuable resource is continued.

Sincerely,
Marilyn Hamill
A Citizen of the United States of America

To Whom it Does Concern,
An email was just sent to me concerning the removal of Social Security Death Index information to genealogists. This infuriates me, first as a citizen born and bred in these American states. To deny information for any reason is outside the vested rights I have as an American. Secondly, immigrants have been coming to the US for hundreds of years. Finding ancestors is of supreme importance to families. Thirdly, governmental control of information, economics, education, business, agriculture, health, et al, tightens the noose that is strangling her once free citizens.

Cease and desist is all I have to say.

Marion Newey
34492 Berg Rd #3
Warren, OR 97053
503 397 5391

I an neither Republican nor Democratic nor any other party since you have all become the same... power hungry enslaving megalomaniacs. You should be ashamed at what you are doing to this wonderful country. A grandmother in Oregon.

January 31, 2012

Dear Committee on Ways and Means,

I totally understand your situation with identity fraud and in how those unfortunate people who have suffered as of result of this, however not everyone is out to steal someone's identity. I am a Genealogical Researcher; the Social Security Death Index helped me in the past to locate family history for my clients. I am pleading with you not to eliminate public access but instead to find a way to limit what is published. My suggestion is to remove the social security number from being published with the Social Security Death Index. There is a downfall to doing this as when a researcher like myself needs to submit a request for other types of research records that require social security numbers, yet there are solutions to help us and to keep the Social Security Number private. In a case scenario such as this perhaps the solution would be that the government is willing to accept our limited information for these records request with just a name, date of birth, and date of death, leaving the government to look up the Social Security Number for that record would aid researchers like me in obtaining such a record. Which are so old that there is no way possible that a identity thief can use that record for themselves or others.

I have been doing my own Genealogical family research for a decade, and because of having the freedom to find a public record such as the social security index, it has helped me to locate several deceased family members, without this resource, it will be impossible to learn important family information. Please find a way to make this work for both of us. Making it private is not the total solution. Do you realize that there are countless other public records that can be had by indemnity thieves? We need to work together on this for better solutions. Thank you for your time in this very important matter, please be sure to include my concerns to your committee before your February 2012 meetings, family history is so very important to myself and millions of others, it is also an occupation for others. It is difficult enough as it is to help others find their families heritage, which pay for the services rendered by Genealogist. This could cost those professional researchers their jobs. Again, please as a Committee work together in finding solutions to benefit both parties and make it possible for millions of people like myself to be able to research, find, and to learn about our family history and heritage. Thank you.

Name - Mary A. Langdon

Address - 2901 Bald Mountain Road

Bear Creek Township, Pa. 18702

Phone number - 570-371-3318

Contact E-mail Address -Emmett1955@gmail.com

Title of Hearing – The Committee on Ways and Means.

February 8, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, **genealogists DO NOT support restricting access to public records that have very little to due with identity theft**.

Currently, four bills are pending in the U.S. Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing U.S. research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,
Megan Peterson
3063 Comfort Rd.
Solebury, PA 18963

Hearing on Social Security's Death Records

Melinde Lutz Byrne, FASG

President, American Society of Genealogists

PO Box 706

Derry, NH 03038

603.247.4775

melinde@melinde.com

Americans are assured that the SSN is not a national identity number. However, for parents to claim dependent children, they must acquire an SSN for each infant . . . or do millions of Americans just make up a number for the 1040? How would anyone know, since no check is made except in extraordinary circumstances? **Principle one**: Use the number as originally intended. Recipients of SSN cards are instructed ON THE CARD not to sign it until they are 18 or have their first jobs. **Solution**: Rescind this part of the IRS Tax Code. Remove SSNs from government birth and marriage records everywhere. Track dependents in a less harmful way. **Result:** Families who tragically lose children are not victimized.

Americans are assured that the SSN may only be required by employers and the IRS, however, Americans are denied loans, driver's licenses, health insurance, medical care, or admission to schools if they refuse to surrender their numbers. These entities who claim a right to living people's SSNs are not required to provide secure storage or to pay damages when SSNs in their care are misused. **Principle two**: End the unnecessary proliferation of SSN requests by entities other than employers or the IRS. **Solution**: Reaffirm that it is unlawful to require a person reveal his or her SSN to anyone but the IRS or an employer. **Result**: Security breaches will not destroy individuals; fraud will not be misdirected onto innocent parties.

Banks and credit companies are particularly irresponsible with SSNs. Past lapses of security have caused immeasurable anguish. **Principle three**: Require audits that review any agency, particularly a bank or credit company to determine whether information is kept securely and that such do not provide backdoors to identity thieves. **Solution**: Prohibit financial institutions from collecting and using SSNs. **Result**: Elimination of this kind of fraud.

Dead people's SSNs can be used fraudulently if these numbers are not accurately published. Employers cannot catch such fraud if the SSDI is inaccurate or incomplete. SSNs are keyboarded by minimum-wage level employees throughout the system. Their work is not proofed. One wrong digit can cause a living person unimaginable suffering. **Principle four**: Ensure the accuracy of reported SSNs for the SSDI. **Solution**: Institute double-entry proofing at all steps in the SSN process. **Result**: Fewer people will become false-positive statistics.

Only through transparency can government function properly. The irresponsible expansion of uses for the SSN has created a nightmare for Americans of a certain age. Worse, misguided agencies have used the SSN for inappropriate purposes, such as Motor Vehicle Registries using SSNs on driver licenses, or State Departments of Health trying to track people from birth to death (EVVE). Maintaining an accurate SSDI for public use is the only way for individuals to protect themselves and for professionals such as private investigators, genealogists, journalists, and medical researchers to conduct reliable research for their clients.

It is inappropriate for bureaucrats to bully law-abiding database providers with threats of retaliation if they continue to provide legally open records. I deplore the tactics used on companies such as *Ancestry.com*.

Dead people do not have more rights than the living. Dead people shouldn't vote – this right can only be protected if deaths are published so poll list supervisors can remove names in a timely fashion. Uses of the SSDI have been myriad. There are thousands of genealogists in America serving hundreds of thousands of clients. Research purposes include medical histories, inheritance rights, historical perspectives, and personal identity issues. Legitimate access should not be curtailed simply because government lacks the flexibility to cope with illegal acts of a very few.

Respectfully submitted,

Melinde Lutz Byrne

MASSACHUSETTS
GENEALOGICAL
COUNCIL

info@massgencouncil.org P.O. Box 5393, Cochituate, MA 01778 www.massgencouncil.org

U.S. Congressman Sam Johnson (R-TX)
Chairman, House Committee on Ways and Means Subcommittee on Social Security
Hearing on Accuracy and Uses of the Social Security Administration's Death Master File
2 February 2012

The **Massachusetts Genealogical Council** (MGC) is an umbrella organization representing more than 36,000 members of genealogical and historical societies who utilize current and historical records to determine kinship. Whether residents of the Commonwealth or descendants of early Massachusetts settlers now living in all fifty states, all wish the Social Security Death Master File (DMF) to remain un-redacted and accessible to the public.

While we are in agreement that there are significant problems within the Social Security Administration's implementation of the DMF, we want to assure that legislation proposed to rectify this problem not have dangerous, if unintended, consequences.

As a tool for research in the genealogical field, the Death Master File is used to determine kinship in a myriad of ways, just a few of which follow.

- As a result of a congressional mandate, the US military hires genealogists to help locate next of kin of servicemen lost in previous wars. In addition, genealogists find DNA donors in each serviceman's family to aid in identification of repatriated remains. The Death Master File is absolutely critical to this research.
- Attorneys and financial institutions employ the services of genealogists in probate, tax and heir-search cases. Again, the DMF is critical to this research.
- Physicians and families use the DMF to locate family members who can supply necessary information to help with diagnoses. Many lives have been saved through donations of blood and bone marrow possible only from family members.

Any bill that attempts to curb identify theft and correct errors within the SSA must not contravene the original reason for the creation of the DMF: to provide a check on identities and assure that the numbers of deceased individuals are not being used fraudulently. The fact that the SSA incorrectly reports deaths of living individuals is a cause for correction of those practices within the SSA, not a complete removal of the DMF.

MASSACHUSETTS
GENEALOGICAL
COUNCIL

info@massgencouncil.org P.O. Box 5393, Cochituate, MA 01778 www.massgencouncil.org

We must do everything we can to stop criminals from profiting from the DMF, but we should not prohibit public access to it. If we are to solve this problem it is essential to first critically examine several points.

1. Countless professions and industries across the nation are ***heavily*** reliant on the DMF: health care providers, the military, financial institutions, attorneys, insurance agencies, universities, funeral directors, credit agencies, and especially state and federal agencies. While exemptions would probably be made for governmental entities, the use of the DMF is now inextricably linked to business practices across the country. Closure of these public records could have severe consequences on the economy as businesses scramble to gather information in other, much less efficient, ways.

2. Tax fraud involving the use of the social security numbers of deceased children results from a lack of communication between governmental agencies. The number of such cases is extremely small, but even those could be eliminated if the IRS were to incorporate use of the DMF themselves. The Death Master File was created, after all, for the purpose of preventing fraud, waste, abuse and identity theft. There really is no excuse for the IRS failing to do the same simple fraud checks the rest of us do. It is extraordinary that victims of this kind of identity theft should be treated as criminals and forced to prove their identities when it is easily within the ability of the IRS to check back a year or two to confirm the correct filings.

3. Rather than enact legislation that is guaranteed to hamper commercial practices across the country, it is preferable to look to within the Social Security Administration itself to correct sloppy procedures that have led to improperly reporting the deaths of living individuals. Improper functioning within the SSA is not a reason to close off access to this tool. First let us correct the mistakes.

4. The Death Master File is **overwhelmingly** used a means to verify identity, not steal it. It is an essential tool for maintaining an open society. In a democratic nation it is our duty to safeguard the right of all individuals to have access to public records, even when there is the chance that those records could be abused. When the records remain open, the fraud is easier to expose.

MASSACHUSETTS
GENEALOGICAL
COUNCIL

info@massgencouncil.org P.O. Box 5393, Cochituate, MA 01778 www.massgencouncil.org

Millions of genealogists would be greatly impacted if legislation restricting access to the DMF were to be enacted. While the Massachusetts Genealogical Council would have preferred to give live testimony at the invitation-only panel at the February 2nd hearing, we submit this written testimony in the hope that our members' voices will be heard. We offer the assistance of our organization to the House Ways and Means Subcommittee on Social Security in safeguarding the security of all Americans with Social Security numbers while promoting open access to public records.

Sincerely,

Polly FitzGerald Kimmitt, CG℠
President, Massachusetts Genealogical Council
P.O. Box 5393
Cochituate, MA 01778
508-842-8850
president@massgencouncil.org

Re: HR 3475

To whom it may concern:

In October 2010 our nine-year old daughter Courtney passed away after a six month battle with an inoperable brain tumor. This was an extremely difficult experience for our very close-knit family and we are still grieving her loss. To make matters worse, we received a letter from the IRS in October 2011 notifying us that someone else had claimed her as a dependant on their 2010 taxes. This caused a significant amount of emotional pain.

Shortly thereafter, we were made aware that her social security number was easily accessible through the Social Security Death Master File as well as on some genealogy sites. We believe this completely unnecessary and is serving to enable criminals to use this information for their own gain at the expense of grieving families, not to mention the money the government could be losing as a result of falsified tax records. We whole-heartedly support this bill.

Mike and Lanaye Burnette
6306 Sunset Drive
Sylvan Springs, AL 35118
205-332-9707
205-919-4688

Michael Diamant, MD
PO Box 1234
Koloa, HI 96756-1234
808-332-9734
mdmd@hawaiian.net

Committee on Ways and Means
Item : Hearing on Social Security's Death Records

On February 2, 2012 at 0900, the Ways and Means Committee will be discussing the fate of the Social Security Death Index records. I am the son of immigrants and currently engaged in a genealogy project. In order for me to accurately reconstruct the personal data for my family, I rely heavily on the SS Death Index records.

I urge the Ways and Means committee to keep these records available to those of us who want to obtain accurate records on their families for the sake of these families, past and present.

Thank you for considering this request.

Michael Diamant, MD
Hawaii

NBER

National Bureau
of Economic Research

James M. Poterba
President and CEO
Poterba@nber.org

16 February 2012

The Honorable Sam Johnson
Chairman, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Xavier Becerra
Ranking Member, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
U.S. House of Representatives
Washington, D.C. 20515

RE: Submission for the February 2, 2012 Hearings on Social Security Death Information

Dear Chairman Johnson and Ranking Member Becerra:

We are writing to describe the substantial value of the Death Master File (DMF) maintained by the Social Security Administration to scholars and policy analysts studying issues relating to population aging and the health and economic status of elderly households. We urge you and your staff to preserve access to the DMF for research purposes, and to restore access to DMF state records that can further enhance health and social science research. Even a brief interruption in the availability of these data could have adverse consequences for a number of significant and ongoing research studies.

The DMF is a fundamental input to the creation of new longitudinal databases that are used in social science research. It is the only way researchers can identify decedents in a timely manner and at low cost - an essential step in large on-going data collection efforts, such as the Health and Retirement Study (HRS). That data set, the HRS, is currently widely used by researchers who study issues such as saving, the demand for and use of long-term care arrangements, and retirement behavior. Dozens of research studies each year rely on the HRS data. The HRS tracks households that were headed by individuals between the ages of 51 and 61 in the early 1990s. The findings from the HRS data analysis are published in leading academic journals and are used in a variety of policy-making contexts.

Tracking vital status -- whether a survey participant is still alive -- is critical in studies of older populations. The DMF is the only source of timely information on death, and with the DMF, it is possible to study the circumstances surrounding death, such as the effects of living near family members or the effect of larger financial asset holdings by the decedent. Because the DMF includes Social Security numbers, it provides a very accurate source of mortality information and it avoids the risk of measurement errors due to incorrect matching between death records and sample survey information. Researchers also use the DMF data to provide a helpful benchmark on self-reported variables in social surveys, such as age. Without the DMF, it would be much more difficult to find objective source of information. This information can be compared with self-reported age to judge the quality of the survey in general.

Researchers at the National Bureau of Economic Research, a non-profit economic research organization that counts nearly twelve hundred academic researchers among its affiliates, are currently using the DMF records to examine the link across generations between longevity and early life circumstances such as birth weight, delivery complications, and parents' socioeconomic status. Understanding the determinants of health and longevity in the elderly population is essential for forecasting future Social Security, Medicare, and Medicaid liabilities. Researchers have used the DMF records to obtain information on death date and last residence for the generations born between 1895 and 1900. They are currently extending this research to the generations born between 1915 and 1919, and a pilot project is currently underway to link generations born in the 1920s, as well their siblings and parents, to the DMF. These projects would be impossible without the DMF. The only other source of the relevant mortality information, the National Death Index, is more difficult to work with than the DMF. It is also much more expensive, and it is less well suited to the research enterprise.

We encourage your Committee to preserve access to the DMF, and to search for ways to balance privacy concerns with the important needs of the research community. We hope that you and the Social Security Administration staff will be able to avoid excluding the research community from DMF access, and that even if there are some limitations placed on DMF access, it will still be possible for researchers to access the information in the DMF for the type of research exercises that we described above. Thank you for your consideration.

Sincerely,

Dora Costa
Director, NBER Cohort Studies Working Group
Professor of Economics, UCLA

James Poterba
President and CEO, NBER
Professor of Economics, MIT

cc: D. Newlon
D. Wise

NATIONAL COUNCIL OF INVESTIGATION & SECURITY SERVICES, INC.

THE NATIONAL VOICE OF THE PRIVATE INVESTIGATION & SECURITY INDUSTRIES

BOARD MEMBERS

President
Maria Vinson Landry

First Vice President
Jim Zimmer

Second Vice President
Robert Heales

Third Vice President
James Huckabee

Secretary
Tom Shamshak

Treasurer
Chris Thornton

Chairman of the Board
Gene Ferraro

Region 1
Neal Holmes Jr.
Larry McWherter

Region 2
Thomas Shamshak
Rosemarie Mesis

Region 3
Ken Cummins
Gregory Carter

Region 4
Bill Pellerin
Steve Sabatke

Region 5
Dean Beers
Bill Butcher

Region 6
Gary Brummond
Neal Custer

Members at Large
John Folino
Jimmie Mesis

EXECUTIVE DIRECTOR
Carolyn S. Ward
7501 Sparrows Point Blvd.
Baltimore, MD 21219
800-445-8408
Fax: 410-388-9746
E-Mail: nciss@comcast.net
www.nciss.org

Statement of Jimmie Mesis, Legislative Chairman

of the

National Council of Investigation & Security Services

Regarding

Social Security Death Records

Subcommittee on Social Security

February 2, 2012

Chairman Johnson, Ranking Member Becerra and members of the subcommittee, I am presenting this testimony on behalf of the National Council of Investigation & Security Services (NCISS). NCISS represents professional private investigators and security officers across the nation.

I currently serve as Legislative Chairman of NCISS. I am a long-time professional private investigator and in addition, I am the publisher of PI Magazine, the profession's largest circulation trade journal.

Private investigators are concerned about legislation, including HR 3475, the "Keeping ID's Safe Act" which would prohibit the Social Security Administration from making information in the Social Security Death Index (SSDI) public. We find that there is a strong public policy value in maintaining public access to the information and that denying access to the SSDI would be counterproductive to the fight against identity theft.

The Department of Commerce's National Technical Information Service (NTIS) explains how the data are used to combat fraud:

"By methodically running financial, credit, payment and other applications against the Death Master File, the financial community, insurance companies, security firms and state and local governments are better able to identify and prevent identity fraud."

Credit granting entities cannot be victimized by anyone using identity information from a deceased person obtained from the SSDI if the firm uses the SSDI to screen applicants. If Congress were to make it more difficult to verify identities, then there would be more, not fewer fraudulent acts. Congress recognized the importance of proper verification of credit applicants when it passed the Patriot Act, which requires depository institutions to adopt "know your customer" processes. Access to the SSDI allows banks and other creditors to have reasonable assurance that an applicant is not using the data of a deceased person to commit fraud.

NCISS members include private investigators and other security professionals who use the SSDI to combat fraud and for other valuable purposes. In addition to helping us fight fraud, the SSN information assists us to narrow our search when looking for lost heirs, or potential witnesses in both criminal and civil trials.

The SSDI is one of the strongest tools in the arsenal used to fight identity theft. When we conduct background checks, due diligence or investigate fraud, the SSDI reveals instantly if someone is using the Social Security number of a deceased individual. It is the best defense we have against the misuse of the identity of deceased persons. A proper use of the SSDI should lead directly to the arrest of identity thieves.

There are other, life-saving uses for the SSDI. In one case I handled, a pharmaceutical company retained me to assist in a drug study. They were not able to locate many of the individuals who had been taking the drug being tested and needed to know if they had died. The SSDI was critical in helping determine the efficacy of the drug.

An essential part of the record is the decedent's Social Security number. It is the key way in which one can distinguish among the thousands of John Smiths listed in the SSDI. Some pending legislation would prohibit disclosure of the Social Security number rather than ban all disclosure. But restricting access to the number would substantially reduce the anti-fraud value of the information in the index. NCISS strongly opposes such efforts.

NCISS would be pleased to provide any additional information to assist the Subcommittee as it considers the pending legislation.

NCOIL
National Conference of Insurance Legislators
...for the states

PRESIDENT: SEN. CARROLL LEAVELL, NM
PRESIDENT-ELECT: SEN. VI SIMPSON, IN
VICE PRESIDENT: REP. CHARLES CURTISS, TN
SECRETARY: REP. GREG WREN, AL
TREASURER: SEN. NEIL BRESLIN, NY

VIA E-MAIL

February 1, 2012

Representative Sam Johnson, Chair
U.S. House Committee on Ways & Means
Subcommittee on Social Security
1211 Longworth House Office Building
Washington, DC 20515

Dear Chairman Johnson:

As leaders of the National Conference of Insurance Legislators (NCOIL), we would like to update you regarding state insurance legislators' activity related to the Social Security Administration's Death Master File (DMF). We recently became aware of your February 2 hearing on the accuracy and uses of the DMF and thought that the Subcommittee should be cognizant of the NCOIL *Model Unclaimed Life Insurance Benefits Act* that relies on the DMF to help ensure that life insurance beneficiaries receive their promised benefits.

NCOIL Past President Rep. Robert Damron (KY) developed the model act in 2011 in response to insurance regulator, state treasurer, and media accounts that life insurance companies would commonly use tools such as the DMF to identify deceased owners of annuity contracts and cease annuity payments, but would not always use those same tools to find deceased life insurance policyholders, for which life insurance death benefits were owed. Rep. Damron believed that stronger company standards were needed to:

- compel routine identification of deceased policyholders
- establish steps for beneficiary notification
- promote timely payment of claims to beneficiaries

NCOIL believes that the model act—which is attached for your convenience—represents an important consumer protection as it serves to ensure the proper payment of policy benefits due to our constituents. NCOIL overwhelmingly adopted the model act following hours of research and debate from legislators across the country and with input from key interested parties.

The NCOIL model, as adopted, requires insurers to quarterly compare the DMF with holders of in-force life insurance policies and retained asset accounts. It calls for timely insurer efforts to confirm an insured or account holder's death, locate any beneficiaries, and provide them with claims forms and instructions. In the event that benefits go unclaimed, the model provides clear procedures for life insurers to notify state treasury departments and to escheat the funds, per unclaimed property laws. Several of the model's provisions, in fact, reflect the terms and business practices of a John Hancock Financial agreement with state treasurers regarding unclaimed life insurance benefits.

NCOIL takes seriously the statements in your hearing announcement regarding incorrect DMF death reports and a potential for identity theft. We agree that correcting false reports and protecting against ID fraud are critical policy goals. Also vitally important is making sure that companies follow through on their promises of payment—particularly to individuals who may have recently lost a loved one.

We appreciate the opportunity to bring our *Model Unclaimed Life Insurance Benefits Act* to your attention as you review DMF-related issues. NCOIL would welcome an opportunity to work with you to ensure that insurance companies continue to have access to important data in the DMF—while protecting against fraud and identity theft, the goal of H.R. 3475, the *Keeping IDs Safe Act of 2011*.

EXECUTIVE DIRECTOR: SUSAN F. NOLAN **NATIONAL OFFICE:** 385 JORDAN ROAD, TROY, NY 12180; TEL: 518-687-0176; FAX: 518-687-0401 **WEBSITE:** WWW.NCOIL.ORG
E-MAIL: INFO@NCOIL.ORG **WASHINGTON OFFICE:** 501 PENNSYLVANIA AVENUE, NW, SUITE 900, SOUTH BUILDING, WASHINGTON, DC 20004; TEL: 202-220-3014; FAX: 202-330-5004

NCOIL is an organization of state legislators whose main area of public policy concern is insurance legislation and regulation. Many legislators active in NCOIL either chair or are members of the committees responsible for insurance legislation in their respective state houses across the country.

For more information, please feel free to contact the NCOIL National Office at 518-687-0178 or our Washington, DC Office at 202-220-3014.

Sincerely,

Sen. Carroll Leavell, NM NCOIL President	Rep. George Keiser, ND NCOIL President (2010-2011)	Rep. Robert Damron, KY NCOIL President (2009-2010)

Enclosures

K/NCOIL/2012/2007631

NCOIL
National Conference of Insurance Legislators
...for the states

Model Unclaimed Life Insurance Benefits Act

Adopted by the NCOIL Executive Committee on November 20, 2011, and by the Life Insurance & Financial Planning Committee on November 17, 2011.

Sponsored by Rep. Robert Damron (KY)

Section 1. Short Title
This Act shall be known as the *Unclaimed Life Insurance Benefits Act.*

Section 2. Purpose
This Act shall require recognition of the escheat or unclaimed property statutes of the adopting state and require the complete and proper disclosure, transparency, and accountability relating to any method of payment for life insurance death benefits regulated by the state's insurance department.

Section 3. Definitions
A. "Death Master File" means the United States Social Security Administration's Death Master File or any other database or service that is at least as comprehensive as the United States Social Security Administration's Death Master File for determining that a person has reportedly died.

B. "Death Master File Match" means a search of the Death Master File that results in a match of the social security number or the name and date of birth of an insured, annuity owner, or retained asset account holder.

C. "Policy" means any policy or certificate of life insurance that provides a death benefit. The term "Policy" shall not include any policy or certificate of life insurance that provides a death benefit under an employee benefit plan subject to The Employee Retirement Income Security Act of 1974 [29 USC 1002], as periodically amended, or under any Federal employee benefit program.

D. "Contract" means an annuity contract. The term "Contract" shall not include an annuity used to fund an employment-based retirement plan or program where the insurer is not committed by terms of the annuity contract to pay death benefits to the beneficiaries of specific plan participants.

Drafting Note: All other terms used in this Act shall be interpreted in a manner consistent with the definitions used in [Insert State Insurance Code].

Section 4. Insurer Conduct
A. An insurer shall perform a comparison of its insureds' in-force life insurance policies and retained asset accounts against a Death Master File, on at least a quarterly basis, using criteria reasonably designed to identify potential matches of its insureds. For those potential matches identified as a result of a Death Master File Match, the insurer shall:

1. within ninety (90) days of a Death Master File Match:

    a. complete a good faith effort, which shall be documented by the insurer, to confirm the death of the insured or retained asset account holder against other available records and information; and

b. determine whether benefits are due in accordance with the applicable policy or contract; and if benefits are due in accordance with the applicable policy or contract:

i. use good faith efforts, which shall be documented by the insurer, to locate the beneficiary or beneficiaries; and

ii. provide the appropriate claims forms or instructions to the beneficiary or beneficiaries to make a claim including the need to provide an official death certificate, if applicable under the policy or contract.

2. With respect to group life insurance, insurers are required only to confirm the possible death of an insured when the insurers provide full record-keeping services to the group policy holder.

3. To the extent permitted by law, the insurer may disclose minimum necessary personal information about the insured or beneficiary to a person who the insurer reasonably believes may be able to assist the insurer locate the beneficiary or a person otherwise entitled to payment of the claims proceeds.

B. An insurer shall not charge insureds, account holders, or beneficiaries for any fees or costs associated with a search or verification conducted pursuant to this section.

C. The benefits from a life insurance policy or a retained asset account, plus any applicable accrued interest shall first be payable to the designated beneficiaries or owners and in the event said beneficiaries or owners can not be found, shall escheat to the state as unclaimed property pursuant to *[Cite state statute for escheat or unclaimed life insurance benefits]*.

Drafting note: Some states' insurance commissioners may want to develop an informational notice that apprises beneficiaries of their rights to the payment of interest on the benefits or proceeds of a life insurance policy or retained asset account. The written notice should be provided by a life insurer to a beneficiary prior to or concurrent with the payment of any life insurance proceeds or the settlement of any life insurance claim, where applicable.

D. An insurer shall notify the *[Insert the state agency for unclaimed property]* upon the expiration of the statutory time period for escheat that:

1. a life insurance policy beneficiary or retained asset account holder has not submitted a claim with the insurer; and

2. the insurer has complied with subsection A of this Section and has been unable, after good faith efforts documented by the insurer, to contact the retained asset account holder, beneficiary or beneficiaries.

E. Upon such notice, an insurer shall immediately submit the unclaimed life insurance benefits or unclaimed retained asset accounts, plus any applicable accrued interest, to the *[Insert the state agency for unclaimed property]*.

Section 5. Unfair Trade Practices

Failure to meet any requirement of this Act is a violation of *[Insert State Unfair Trade Practices Statute]*.

Drafting note: Some states' Unfair Trade Practices statutes specify that an act must be shown to be a "pattern" or "general business practice" in order to constitute a violation of that statute. In those instances, care should be taken in the adoption of this model to ensure consistency across those two statutes.

Section 6. Effective Date
This Act shall take effect on or after *[insert appropriate date]*.

Drafting note: To address other concerns with transparency and accountability in life insurer procedures relating to treatment of retained asset accounts, please refer to the NCOIL Beneficiaries' Bill of Rights, which requires extensive written disclosures to consumers and insurer reporting.

K:/NCOIL/2011documents/2007511e.doc

NATIONAL GENEALOGICAL SOCIETY

3108 Columbia Pike, Suite 300
Arlington, VA 22204-4304

703- 525-0050 800- 473-0060
Fax 703-525-0052

STATEMENT FOR THE RECORD, HOUSE COMMITTEE ON WAYS AND MEANS, SUBCOMMITTEE ON SOCIAL SECURITY, WRITTEN COMMENTS ON PROVISIONS RELATING TO SOCIAL SECURITY ADMINISTRATION'S DEATH MASTER FILE.

I. INTRODUCTION

House Committee on Ways and Means, Subcommittee on Social Security held a Hearing on 2 February 2012, regarding the accuracy and uses of the Social Security Administration's Death Master File. No one from the genealogical community was invited to testify at the hearing, but we were invited to submit a written statement. This statement is submitted on behalf of the National Genealogical Society.

II. BACKGROUND ON THE NATIONAL GENEALOGICAL SOCIETY AND CONTACT INFORMATION:

The National Genealogical Society (NGS) is a non-profit Virginia corporation, founded in 1903 and has approximately 9,000 individual members and 650 organizational subscribers which include regional, state, and local societies. Although our membership includes many professional genealogists, most of our members are people actively researching their own families. All officers and directors serve as volunteers and receive no compensation for performing their duties.

The mission of the National Genealogical Society is to serve and grow the genealogical community by providing education and training, fostering increased quality and standards, and promoting access to and preservation of genealogical records.

The genealogical community works together through The Records Preservation and Access Committee (RPAC), a joint committee which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS), and the International Association of Jewish Genealogical Societies (IAJGS) as voting members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), and the American Society of Genealogists (ASG) also serve as participating members. RPAC also includes participation from a few of the commercial providers of genealogical information. RPAC meets monthly to advise the genealogical community on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

Contact information: Janet A. Alpert, National Genealogical Society, 3108 Columbia Pike, Suite 300, Arlington, Virginia, 22204-4304, telephone 703-525-0050, fax 703-525-0052, and email janalpert@aol.com. Janet A. Alpert is a member of the National Genealogical Society board of directors, immediate past president, and served two terms as president from 1 October 2006

through 30 September 2010. She previously served one term as secretary from 2004 through 2006. Ms. Alpert has a Bachelor of Arts Degree in Political Science from the University of California, Santa Barbara, California, and a Masters in Business Administration from the University of Connecticut. She retired in 2004 from a thirty-five year career in the title insurance industry, and now resides in Hilton Head Island, South Carolina. Ms. Alpert is an amateur genealogist who has been researching her family for over thirty years.

III. OVERVIEW OF THE ISSUES

The Social Security Administration's Death Master File (DMF) is a publicly available resource of great value to both family history researchers and professional genealogists. Genealogists use a commercial version of the product called the Social Security Death Index (SSDI). The SSDI has been available to the public since the Consent Judgment, Perholtz v. Ross, No. Civ. 78-2385, Dist. D. C. (April 3, 1980).

Genealogy is different than the other social sciences where researchers draw their conclusions from a broad overview of the available records. Genealogists study specific individuals—their ancestors. Therefore if a genealogist does not have access to the records about the ancestor they are researching, their work may come to an abrupt halt.

I am writing on behalf of the National Genealogical Society, its members, and organizational subscribers about why family history researchers and professional genealogists need access to the Social Security Death Index (SSDI).

1. Many genealogists begin researching their family because there is a part of their family they never knew. The estrangement may have occurred because of adoption, divorce, abandonment, death, or other reasons. Regardless of the cause, learning about an unknown branch of the family helps the healing process. The SSDI has been an essential tool for genealogists looking for relatives who were born in the 19th and 20th centuries.

   From the earliest settlements in America, we have been people on the move, generally migrating west in search of cheaper land and better opportunities. Since Vital Records are kept by state, without the SSDI, no national index will be available to determine where people might have moved. Information contained in the SSDI includes the state where the social security number was initially issued and the social security number, which helps genealogists determine if this is the actual person they are researching. After finding the person in the SSDI, the researcher often writes to the Social Security Administration, OEO FOIA Workgroup, P.O. Box 33022, Baltimore, Maryland 21290-3022 for a copy of the original Social Security application form, called the SS-5. The SS-5 contains valuable information for family history researchers including full name at birth including maiden name, date and place of birth, current address, and full name of father and mother. The SS-5 is necessary if you are researching someone with a common

name, to make sure you identify the correct parents. The researcher pays a fee of $27 for a copy of the SS-5, and a fee of $29.00 if we do not have the Social Security number.

2. Another use of the SSDI is to find the date of death and location of the person you are researching so you can look for an obituary. Many recent obituaries are available online, but many older obituaries are on microfilm and obtained by writing the local library for a copy. Librarians cannot do an extensive search, but can usually find an obituary if they have the death date. An obituary normally identifies living and deceased relatives, the married names of daughters, and the current cities of residence which is essential information.

3. A third use of the SSDI is to find siblings and cousins when a family carries a disease which can be inherited. In these instances time is of the essence. The first step is to find the aunt or uncle, or great aunt or uncle in the SSDI, and then follow the procedure in (III. 2.) above to locate their obituary. Finding and notifying distant cousins can mean the difference between early detection and treatment versus possible death.

   Each year since 2004, the Surgeon General (see http://www.surgeongeneral.gov) has declared Thanksgiving to be "National Family History Day." When families are together over the holidays or at other gatherings, the Surgeon General encourages families to discuss and write down the health problems that appear to run in their family and to share the information with their family doctor. The Health and Human Services website http://www.hhs.gov/familyhistory/ provides a "My Family Health Portrait" tool for families to record their health history information.

   Diseases residing in estranged branches of the family as described in paragraph III.1. above are sometimes the silent killers. Parents of adopted children are given the health history of the biological parents. However, since the biological parents are often under the age of thirty-years old, sometimes there are few health risks disclosed. If you could ask those same parents about their health history fifty years later, after their parents have died, the answer would be more complete. Therefore it is important for people who are adopted to first identify and then reach out to their biological parents and siblings after they reach adulthood.

4. Professional genealogists need access to the SSDI to continue their livelihood. You can learn more about the Association of Professional Genealogists (APG) which has over 2,000 members in the United States at http://www.apgen.org/about/index.html. In addition to helping clients discover their family history, many professional genealogists have important specialties.
   a. Some professional genealogists work in the field of forensic genealogy. Working with the military they help find the families of servicemen lost in previous military conflicts to assist in the repatriation of the remains.
   b. Others work with county coroners to identify the relatives of unclaimed persons.

c. Some clients include attorneys who need to find missing heirs to settle estate cases.
d. Other genealogists specialize in finding the living biological parents or siblings of someone who was adopted.

It has been suggested that professional genealogists could use LexisNexis for their research in lieu of the SSDI. Subscriptions to LexisNexis are cost prohibitive for self-employed professionals. The cost to provide the above professional services will go up if the SSDI is no longer available in the future.

IV. SOLUTIONS AVAILABLE TO SOLVE IDENTITY THEFT OF DECEASED INDIVIDUALS

Genealogists are also opposed to identity theft and support efforts to stop it. We believe the current laws and regulations provide a means to stop identity theft RIGHT NOW, if government agencies use tools which are already available.

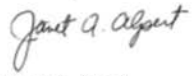
1. If income tax returns were electronically compared to the Master Death File, the income tax return of a deceased individual could be flagged for special processing, thus thwarting the person attempting to create a tax fraud before the fraud occurs.

2. The SSNs of parents should be required when filing a tax return for any minor. If the minor dies, the IRS could have a procedure to flag any filings without the parents' social security numbers, again preventing attempts at fraud.

3. The National Taxpayer Advocate's report for 2011 specifically highlights the benefits of the IRS Issued Identity Protection PINs and suggests that taxpayers should be allowed to turn off their ability to file tax returns electronically. When there is a death in the family, the executor needs the ability to turn off the electronic filing ability.

We feel strongly that the hearing on 2 February 2012 incorrectly portrayed genealogists as the cause of fraud. By not inviting a representative from the genealogical community to testify, you failed to allow an open discussion on the real causes of tax fraud and constructive ways to prevent it. We appreciate the opportunity to present our positions to the subcommittee.

Sincerely,



Janet A. Alpert
Immediate Past President of the
National Genealogical Society and
NGS Representative on RPAC

February 1, 2012

Committee on Ways and Means

re: Hearing on Social Security's Death Records

To Whom It May Concern:

Being a victim of identity theft, I strongly oppose fraud and identity theft! With that said, I also want to show my support for continuing making public Social Security's Death Master File. I am a professional genealogist and private investigator, the SSDI is extremely useful in my profession. Taking the SSDI away from the public and not making it accessible for genealogical or investigative purposes would literally make our research go back 100 years. Yes, there will always be criminals taking advantage of this type of information but they can find this info anyway. All they have to do is read the local newspaper or online obituaries, drive by a cemetery, or go to the county probate office where files are public record and obtain copies of whatever documents may be in a deceased's individual file such as a death certificate (which includes SSN, date and place of birth, mother's maiden name, and even the address to their last residence) or petition listing the heirs and their social security numbers!

The reports you were previously given list the abuse that the public has endured due to the SSDI. Let me mention a few of the beneficial aspects of a public SSDI:

1) private investigation cases for civil and criminal matters
2) heir research for probate matters
3) genealogical research performed by professionals
4) personal family research performed by individuals
5) adoption research performed by individuals

There are 12,074 private investigation companies in the United States, with annual business sales of $100M-$500M. Include heir locaters, genealogical researchers and genealogical-based companies, and you can easily double those numbers.

I strongly urge the members of the committee NOT to remove Social Security's Death Master File from public use. Unfortunately, I believe that Chairman Sam Johnson in his effort in trying to do something good for Americans, is doing something bad. Thank you for considering my opinion in this matter.

Patricia A. Champion
Champion & Champion
14207 Emerald Hill Drive
San Antonio, Texas 78231
Tel: (210) 408-1180 Fax: (210) 408-1188
E-mail: trish@champion-champion.com

Hearing on the Social Security Death Records

Name: Patricia Stinson
Address: 1552 Moon River Drive #5
Provo, Utah 84604
Phone: 801-356-1002
Email: cotostinson@hotmail.com

It has come to my attention that there will be a hearing on the Social Security Death Records to determine, among other things, if access to them should change. I understand that this change is being considered because of identity thief. Even though I support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft, I feel that limiting or stopping access to the SSDI would be wrong and ill advised.

Limiting or stopping access to the SSDI would have an adverse effect on the income of those that depend on these records to do their jobs. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, genealogists and others. In a struggling economy, Congress should not consider actions that would negatively impact workers, when the action does not accomplish the intended good.

Limiting or stopping access to the SSDI would actually increase identity theft because it verifies a person's death. Persons wishing to commit theft would still steal identities of individuals who have passed away by reading the obituaries in local newspapers (which are online for most), and then conduct business in another state. Without the SSDI, a national database to check, it is extremely unlikely other states would be aware of the death. In the end it will not stop theft, but in all likelihood increase it.

Limiting or stopping access to the SSDI would make it more difficult or impossible for families to access important family information. There are mental and physical health issues that are hereditary. Although the SSDI does not have this information, it helps researchers locate death information that can lead to family medical histories.

Limiting or stopping access to the SSDI would adversely affect the millions of genealogy researchers, and the good produced by it. Genealogy is more than a fun or benign hobby**.** Genealogists gain an education as they pursue their family history. They gain knowledge about history, culture, languages, paleography, geography, law, institutions, government. They gain greater understanding not just of their families, but politics, institutions, and communities, and the impact of decisions made by individuals and governments. This makes them more informed voters and citizens.

In addition, genealogy addresses many of the problems in our society due to the disintegration of families and communities, high mobility, economic downturns, isolation, and a host of other challenges. People learn from the experiences of others in history. It takes on added meaning because it is their family.

Finally genealogy research, which relies on records like the SSDI, helps people to understand more about themselves. People are in a large measure a product of their family and environment**. Withholding**

information, like that in the SSDI, from people, is in effect robbing them of their identity. So you could say that you will be helping to perpetrate another form of identity theft.

I say this from personal experience, having pursued family history for over twenty years, and more recently having completed a degree in family history and genealogy. I understand how seemingly small decisions by the government can lead to big outcomes for individuals.

I hope that in your upcoming hearing you will not limit or stop access to the SSDI because I believe that what you hope to gain will only lead to more identify theft, by those committing the crime, and on individuals who are searching for their identity. This is in addition to an adverse impact on income for those who use the records in their jobs.

Sincerely,

Patricia Stinson

Regarding HR 3475, Keeping IDs Safe Act of 2011:

My name is Patricia P. Wales.

I am an amateur genealogist.

My address is 3311 West 92nd Place, Westminster, CO 80031

My phone number is 303-426-6669

My e-mail address is patpwales@hotmail.com

The title of the hearing on which I wish to submit comments is HR 3475, *Keeping IDs Safe Act of 2011*

My comments are:

Please do not enact this misguided bill. It is another example of heavy-handed legislators throwing out the baby with the bathwater, using the excuse that it is necessary to protect IDs.

There are many reasons to keep the SSDI available for all. I am an amateur genealogist and since I never met my Grandparents and Great-Grandparents I, like many other genealogists, have found the SSDI essential for locating when and where they lived and died.

The Social Security Numbers in the SSDI are not what genealogists need; it is the date and location of a relative's death that is important to us. Perhaps there is a middle road that makes the SSDI available but excludes SSNs from it.

Thank you for your consideration of the concerns of genealogists in a matter of great importance to us.

Friday, February 3, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Raphael M. Whelan
3990 18th Street Apt. #1
San Francisco, CA 94114-2592

U.S House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Records Preservation & Access Committee
Federation of Genealogical Societies, National Genealogical Society,
International Association of Jewish Genealogical Societies

Statement for the Record

Hearing on Social Security's Death Records

Submitted by

Frederick E. Moss, JD, LL.M.

February 2, 2012

Chairman Johnson, Ranking Member Becerra, and members of the Subcommittee.

Thank you for the invitation to submit this Statement for the Record on behalf of the genealogical community through its Records Preservation and Access Committee to supplement the record of the hearing held by the Subcommittee on the 2nd of February 2012.

I serve as the legal advisor to the Federation of Genealogical Societies and as a member of the Records Preservation and Access Committee more fully described below.

Be assured that the genealogical community shares the objective of protecting Americans against fraud and of addressing deficiencies in the current operation of the Social Security Administration's Death Master File. This hearing marks our first opportunity to express our views to Congress on this important subject and we commend the committee for adding it to their agenda.

Egregious Identity Theft Cases Can Be Stopped Using Existing Resources

We have all been outraged by reports of identity thieves filing fraudulent tax refund claims using the SSNs of recently deceased infants & adults. Our strongest message is that the means to stop this particular form of identity theft exists now, without waiting for any additional legislation.

The Internal Revenue Service could curtail such claims almost immediately if tax refund claims were screened against the SSA's Death Master File & matching cases identified for special processing. This filter, together with other viable and easily implemented safeguards, could actually expedite the processing of such claims.

The National Taxpayer Advocate (in her 2011 Report referenced by the Chairman in announcing this hearing) has also endorsed the use of IRS- issued Identity Protection PINs and allowing taxpayers to turn OFF the ability to file tax returns electronically using specified SSNs. See pp. 61-62.

The resounding message we heard from the Operation Rainmaker press conference convened by the Tampa Chief of Police, was that the online tax refund system is unacceptably vulnerable, has been corrupted, and that there are identity thieves fully aware and anxious to exploit the weaknesses in that system. http://www.tampabay.com/news/publicsafety/crime/49-accused-of-tax-fraud-and-identity-theft/1189406

There's no need to wait for legislation to stop this travesty and protect families of deceased infants and adults. What is required is for the IRS to use the SSA's Master Death File for the fraud prevention purposes for which it was originally created.

Public Access to the Death Master File

Congressman Marchant posed a question raised by a constituent (and "millions like her") when he asked how we could be careful in what we do so that the people who are harmed are protected but those vitally interested in their ancestry can still access accurate information.

We followed with great interest Commissioner Astrue's progress report on the Office of Management and Budget's efforts to arrive at a coordinated administration position concerning appropriate public access to the Death Master File. His observation was that the issues are more complex that they might at first appear and that an attempt to rush a decision would almost surely get it wrong. We support a thorough review of these issues and would urge decision makers not to leap to solutions before the problems have been carefully defined and options developed.

What has been missing from the process so far has been input from actual genealogists. It is impossible to "balance" competing interests if representatives of one side cannot "add weight" to their side of the balance scale. If given an appropriate opportunity to make the case, we are confident that public access to the DMF for legitimate genealogical purposes can be justified.

The Records Preservation and Access Committee is prepared to assist in providing that input by coordinating the appearance of highly qualified, well-recognized representatives prepared to provide information to assist decision-makers in the Executive and Legislative branches in making well-informed decisions.

Interests of the Genealogical Community

The interests of the genealogical community are not hard to understand. Access to records or the lack thereof, is the pivotal issue for genealogists. Without documentation, our family histories are more legend than history. Recent genetic advances have given additional significance to well-documented medical family histories. You can expect to hear expressions of concern from across the genealogical community whenever they may have reason to believe their access to these records is being threatened.

About the Records Preservation and Access Committee

The genealogical community works together through The Records Preservation and Access Committee (RPAC), a joint committee which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS) and the International Association of Jewish Genealogical Societies (IAJGS) as voting members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), the American Society of Genealogists (ASG), and industry representatives also serve as participating members. RPAC meets monthly, and more often if needed, to advise the genealogical and historical communities, as well as other interested parties, on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

Summary

We offer two main points:

(1) Our strongest message is that the means to stop this particular form of identity theft exists now, without waiting for any additional legislation.
(2) As existing policy regarding public access to the Death Master File is reviewed, we urge that input from actual genealogists be sought. The members of the Records Preservation

and Access Committee stand ready to assist in arranging for that input to both the Executive and Legislative branches.

FROM: Ruth Sevier Foster
1244 Arbor Rd. #512
Winston Salem, NC 27104-1148
336-723-0946

I took the time to write this to you… and I vote.

Please do not make changes in access to the Social Security Death Index as this is non-threatening and absolutely of beneficial use for all of us GENEALOGISTS. Rarely, has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises.

ealogists support Congress's intent to protect Americans from improper usage of

• **Genealogists** doing US research located both in and outside the United States rely on the Social Security Death Index (SSDI), which is the commercial name of the Death Master File (DMF). The Death Master File is a computer database file made available by the United States Social Security Administration since 1980.

• SSDI is a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death MasterFile (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. In addition to family history researchers, the SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs inprobates, media reporters, university researchers, and others.

• Genealogy is a hobby for millions of people. A study from May 2009 3 characterizes those individuals interested in genealogy as follows:

49 million feel a deep appreciation for their ancestors*

13 million are active researchers**

More than 8.5 million visited genealogy-oriented sites in the last month (excluding search engines and long-tail sites).***

9 million are hobbyists**

1.6 million online adults 18-44 consider genealogy a hobby (3%)

7.5 million online adults 45+ report genealogy a hobby (8%)

A total of 9.1 million total hobbyists (out of an online universe of 148 million 18+)

• Genealogy also is a serious profession.

• Genealogists use the SSNs to appropriately identify records of people when tracing **family medical history**, especially if the person has a common name: Sara Cohen,Tom Brown, Jose Martinez, Trung Lee, etc. Genealogy assists in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members.

The SSN is critical to make certain that one has the correct person.. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family4. Information on three generations is thesuggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative5.

• Genealogists work with coroners to find next of kin for the deceased. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See unclaimedpersons.org

• Genealogists work with military to locate relatives of soldiers who are still unaccounted for from past conflicts. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family.

• Other stakeholders who are concerned and want full and immediate access to the SSDI include: the financial and insurance industries [they need the information timely so that they can verify deaths to pay out death claims and verify beneficiaries for paying retiree benefits]; federal, state and local law enforcement agencies; Lexis-Nexis; charities legacy departments and planned gifts departments, medical researchers [tracking morbidity cluster deaths and tracking mortality of medical trial results]; state, county government and teacher retirement funds; county assessment offices, student loan companies; universities for student loans, tracing alumni mortalities and other activities, enhanced collections department of state courts, and other stakeholders that we are learning about daily.

On behalf of Savannah Area Genealogical Association, I urge you to **Please keep the Social Security Death Index available to everyone.**

Genealogy hobbyists and professionals need the Social Security Death Index."

- Information provided by Social Security Death Index helps reunite families of MIAs and KIAs with the remains of their loved ones.

- Frequently, the information found in SSDI, verifies a family tie that is needed for genetic medical conditions.

- If banks and other businesses were doing their jobs properly, the misuse of Social Security Numbers would not be an issue. The numbers in SSDI would help them prevent identity theft.

Honey Ryan
Vice President, Programs
Savannah Area Genealogical Society
11 Marsh Point Drive
Savannah, GA 31406
Home: 912-356-1488
Cell: 912-657-6806
hryansavh@aol.com

3 Feb 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Sandra Miarecki
1545 Delaware St
Berkeley CA 94703

16W668 Marybeth Court
Burr Ridge, Illinois 60527
January 30, 2012

Dear Members of the House of Representatives:

Re: HR 3475, Keeping IDs Safe Act of 2011

HR 3482 To prevent identity theft and tax crimes.

HR 3215 To prevent identity theft and tax fraud

I am writing to ask that you do not eliminate or curtail the use of the Social Security Death Index through the internet. I understand that some people feel that having this information available to the public invites identity theft.

Most Social Security numbers get into the possession of the wrong person due to computer breaches into government and/or corporate databases.

Having the SSDI on line, allows companies identity Social Security numbers that belonged to individuals who are now deceased, such as insurance companies, stores, and medical researchers.

Over 9 million U.S. citizens are actively engaged in researching their family history as a hobby and others as a profession. The SSDI is a rich source of information for these individuals. Unhappy genealogists will remember this at election time.

Yours truly,

Sandra Trapp
630-325-0799
swt39@juno.com

Subj: Submission regarding pending legislation regarding the Death Master File (DMF)
Submitter: Scott S. Shenton
Organization: self
Address: 2725 N. Highway A1A #301, Indialantic, FL 32903

I have been a serious amateur genealogist for over 15 years, researching my Shenton ancestors and all who bear the Shenton surname. While I am not a professional genealogist, I am a member of a local genealogical society, have been a member of several societies in areas where my ancestors lived, actively maintain several different web sites specifically focused on various aspects of my research, and correspond regularly with dozens of like-minded researchers and people newly interested in learning about their family history.

Many people new to genealogy and family history have been spurred in their interest by current television series such as the popular 'How Do You Think You Are'. When they first start out on their searches, one of the earliest sources they find is the Social Security Death Index (SSDI), the commercial version of the Death Master File (DMF). One of the basic principles taught to 'newbies' is to 'start with what you know, and work backwards'. Obviously, what people know best is their immediate family – parents and grandparents. And the best sources for information on parents and grandparents, which usually leads to information on earlier ancestors, is the Census and the SSDI.

It would be a major disservice to 'newbies' and to all researchers to remove the SSDI from public access or severely reduce the amount of available information. I can certainly understand the concerns about the SSDI – both as they relate to the possibility of its use for fraudulent tax filings, and to inadvertent posting of erroneous death information. However I have been, in both my professional career and personal life, heavily involved in the use and development of computer systems, and both issues (tax and privacy) appear to be obvious applications for improved computer technology:

- The Internal Revenue Service, with modest improvements in computer programs, internal work procedures, and – if necessary – additional legislation, should be able to utilize the DMF/SSDI to detect and stop virtually all fraudulent use of Social Security Numbers, wherever they might have been obtained.
- The Social Security Administration, also with modest improvements in computer programs, internal work procedures, and – if necessary – additional legislation should be able to significantly reduce the already minor error rate of invalid entries in the DMF/SSDI.

Given such successful reduction of the opportunity for fraud and error, additional consideration should be given to the fundamental issue of identity theft, whether against the IRS or private citizens, and making the definition of such criminal activities more clear and with more explicit penalties.

In short, please consider addressing targeted solutions (better computer processing, better work procedures, and – if necessary – specific legislation) instead of the shotgun approach of information suppression.

To: Committee on Ways and Means
From: Sean Furniss
11094 Saffold Way
Reston, VA 20190
703-481-5899
Sean.Furniss@gmail.com
Hearing on Social Security's Death Records

This letter is written in response to the Chairman Sam Johnson's announcement of a subcommittee hearing on the accuracy and uses of the Social Security Administration's Death Master File to take place on 2 February 2012.

The very limited opportunity for groups and individuals to present testimony for the administrative record for the hearing is lamentable. Given the extensive time periods that Congress makes Federal agencies provide the public to review and comment on documents and regulations, one would think that members of the Ways and Means Committee would be the first to understand the need for sufficient amount of time to review, understand and discuss proposed legislation in an open forum.

While Congress is very clear in mandating that Federal agencies use simple English to provide a clear and precise understanding of proposed regulations, the information provided by the Committee related to the proposed bill (HR 3475) fails to provide a clear and precise understanding of the full effects of what would happen under this bill if it were to actually pass and be signed into law.

Congress needs to focus on measures that will target the criminal activities, improve interagency cooperation, improve the tax refund process, and provide the Social Security Administration sufficient funding to address any deficiencies in maintaining the DMF and not just think that eliminating public use of the DMF would solve everything at no cost.

Of the three House and one Senate bill drafted to address problems with the quality and maintenance of the Death Master File (DMF), HR 3475 is clearly the most seriously misdirected of the proposed legislative proposals.

HR 3475 does not clearly address what the Committee believes is needed to be accomplished nor use the best, most effective way to do so. HR 3475, as it is currently written, would effectively end general public access to the DMF. The thinking that this legislation would improve the quality of the DMF and reduce crime appears muddled and confused.

The thought that access to the social security numbers of all dead individuals with social security numbers (not just dead American taxpayers as stated by Chairman Johnson) is a significant cause of identity theft and that keeping social security numbers of "deceased" individuals from being public would help reduce

the erroneous entry of the numbers of living individuals in the database by the Social Security Administration is unfounded in fact.

Rarely has it been documented that the information in this database has been used to for identity theft. If the Committee truly thought that identity theft is a critical issue, then perhaps some thought should be given as to how to better protect the personal information that has been routinely stolen from government and corporate databases (over 500 million stolen according to a 2009 report).

Among the problems with including and resolving problems of having living individuals included in the DMF is an inadequate level of funding and error checking at all levels of government. Without adequate human resources and computerized cross-checking errors within the DMF can not be realistically addressed in an efficient manner.

The information in the DMF is used to create the Social Security Death Index which is used by financial and insurance industries, law enforcement agencies, medical researchers, retirement funds, tax assessment offices, loan companies, courts and many others.

Additionally over 9.1 million Americans make use of the information from the DMF to trace their family histories and create medical histories. Reliable medical family histories are increasing requested by medical professionals at all levels of practice.

I urge the members and staff of the Committee to reassess what needs to be accomplished and to develop a more reasonable and practical method to address those needs.

Thank you for this opportunity to comment on the proposed legislation.

Sean Furniss
11094 Saffold Way
Reston, Virginia

Hearing on Social Security's Death Records
1 February 2012
Selma Blackmon
2200 Willowtrail Pkwy lot F3
Norcross, GA 30093
770-931-2609
sbgenealogy@gmail.com

This statement is to be attributed to Selma Blackmon

The following is a very brief note I posted on Examiner.com on 1 February 2012.
As the last paragraph demonstrates, the SSDI is very important for research. Without this tool, the deceased military father would not have been located. Other research attempts did not narrow the search for a specific person. The family did know the approximate death date and military history. The family did not know the exact death date or location. Three businesses offer access to the SSDI. Changes in access will affect these businesses as well as genealogical research. Genealogy is the second largest hobby. Family history research online and on location stimulate our economy.

Genealogy: Social Security Death Index (SSDI)

Genealogists acquire unknown family information using the Social Security Death Index. (SSDI). The family historian may find a death date, death location, clues for obituary or cemetery research. This information will lead the historian to the "how and where" to order a copy of the death certificate.

The SSDI was created from the Social Security Administration's Death master file. The index with related information is available on:
Ancestry.com {www.ancestry.com] includes searching tips, FAQ, and how to write an application request letter to the Social Security Administration.
Family search.org {www.familysearch.org], a free site, includes wiki information on the collection time period, description, and content.
[https://www.familysearch.org/learn/wiki/en/United_States_Social_Security_Death_Index_(FamilySearch_Historical_Records)]
Genealogybank.com [www.genealogybank.com] offers a free printable search results with suggestions to their fee site for obituaries and historical newspapers. The obituary and historical newspaper search is free; access to the articles is fee based.

The SSDI includes deaths reported to the Social Security Administration (SSA) beginning about 1962. Not every death is included. Sites for more information:

The Social Security Death Index: A Genealogy Records Guide by Joe Beine [http://www.deathindexes.com/ssdi.html]

Roots Web's Guide to Tracing Family Trees, Guide No. 10. *A Unique Finding Aid: Social Security Death Index (SSDI) and Railroad Retirement Board Records* [http://rwguide.rootsweb.ancestry.com/lesson10.htm]

"Social Security Sleuthing" offered by The National Genealogical Society consists of five lessons on a CD. [www.ngsgenealogy.org/cs/socialsecurity_sleuthing]

Tears flowed. "This helps me see him as a living person. This makes him real to me." This reaction occurred from a family member who had never met his/her father. The father served in WWII and died in mid-1950. After looking online for the digitized SSDI information, the exact date and location were found. With this information, an online digitized Texas death certificate was printed. Tears of joy flowed as this family member went away to share new information with other family members.

Thank you for understanding the need to continue to offer this valuable research tool.
Selma Blackmon

STONE HOUSE HISTORICAL RESEARCH
Catherine B. W. Desmarais, Professional Genealogist℠

399 Old Stage Road
Essex Junction, Vermont 05452
stonehouseresearch@gmail.com
802-363-7885

30 January 2012

RE:
Please oppose
• HR 3475, Keeping IDs Safe Act of 2011
• S 1534, the Identity Theft and Tax Fraud Prevention Act
• HR 3482 To prevent identity theft and tax crimes.
• HR 3215 To prevent identity theft and tax

Dear Congressmen and Congresswomen:

I perform research, through SNA International, for the Department of Defense related to the congressional mandate to repatriate the remains of unaccounted-for service personnel. The majority of these are from World War II and the Korean Conflict. My research identifies and locates the primary living next of kin and the family members eligible to provide DNA Family Reference Samples to aid in identification of remains. I could not effectively conduct this research without free access to the Death Master File – Social Security Death Index (SSDI). Many of these servicemen and most of their parents were born before universal vital records registration. The mid-twentieth century was a time of increasing migration of families, and the SSDI is very often the only resource available to trace the serviceman's deceased relatives in order to find their living descendants. I believe that the tiny number of cases in which the SSDI was misused is far outweighed by the positive effects it provides to bring closure to the families of those who gave their lives for our freedom.

Likewise, I also use the SSDI in my research cases for attorneys to locate the heirs and next of kin in probate and title insurance matters. For example, the SSDI allowed me to trace the deceased siblings of an elderly woman who died subsequent to Alzheimer's disease, and locate her living great-nieces and great-nephews who had the right to be notified about her estate. This research reunited a family that had lost contact with each other in a previous generation. In another case, a property owner discovered that they did not own clear title to their front yard. The SSDI allowed the identification of the next of kin of the former property owner, now long deceased, so that the title could be repaired. All of this research would become impossible or, at best, significantly more expensive and time-consuming if the SSDI was not freely available. In closed-records states, the SSDI may be the only source that meets Rules of Evidence to document deaths to the satisfaction of the courts.

The SSDI was designed to prevent identity theft and fraud. Rather than eliminating it, its use should be strengthened so that banks and the IRS are required to cross reference social security numbers with the SSDI to assure that a deceased person's number is not being reused. Making it inaccessible or difficult (and expensive) to access would be counter-productive and would prevent all the positive outcomes for which it is used today.

Loss of public access to this irreplaceable resource will have many negative financial, legal, and human costs. I *oppose* the bills listed at the top of this letter. Thank you.

Sincerely,

Catherine W. Desmarais, Certified Genealogist
Owner, Stone House Historical Research

Sunshine in Government Initiative
1101 Wilson Boulevard, Suite 1100 · Arlington, Virginia 22209
Phone (703) 807-2100 · info@SunshineInGovernment.org

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
1129 Longworth Bldg.
Washington, D.C. 20515

The Honorable Xavier Becerra
Ranking Member
Subcommittee on Social Security
Committee on Ways and Means
1139E Longworth House Office Building
Washington, D.C. 20515

Re: Submission of media coalition written comments on February, 2, 2012, "Hearing on Social Security Administration's Death Records."

February 16, 2012

Dear Chairman Johnson and Ranking Member Becerra,

We are writing add a media perspective on the public uses of information in the Social Security Administration's Death Master File (DMF). **The Sunshine in Government Initiative** is a coalition of media associations promoting government transparency.

We request our statement be included in the record of the February 2, 2012, hearing entitled, "Hearing on Social Security Administration's Death Records." In its efforts to address concerns about identity theft, Congress should preserve the availability of information that reporters have for decades used to inform the public about important issues.

First, we commend the Committee for holding the public hearing on proposed changes to public access to the Death Master File. Too often decisions affecting what the public can find out from and about their government are made without adequate public discussion. When there is public debate, frequently it occurs late in the legislative process. Early public discussion about any proposal to add to the more than 240 laws already on the books that limit FOIA's reach serves the public well, and we appreciate the opportunity to contribute to this discussion.
Journalists have used the DMF in a number of stories that contributed to the public interest. Here are some examples:

- In 2005, the Birmingham News used the Death Master File to identify factory employees add a human element to a story on factory workers in an investigation of asbestos exposure and mesothelioma.

- Dead people are listed on voter rolls and some voted in 2003, *The Times of Northwest Indiana* showed dead people still listed on voter rolls. This case is not isolated. Years

earlier, also using the Death Master File, the Ashbury Park Press in September 25, 1994 reported dead people voting in Ocean City, New Jersey.

- The Scripps-Howard News Service documented the red tape nightmare facing relatives of dead people whose identities are stolen using the Death Master File. Scripps-Howard presented the issues without publishing the social security numbers themselves.

Any adjustments to public access to the DMF should allow journalists' continued responsible use of the Death Master File to inform the public. We recognize the concern about preventing thieves from using the DMF to falsely claim tax deductions. At the same time, access to the information in the Death Master File is vital to keeping the public informed. We believe it may be possible to address concerns about identity theft while preserving public access to the Death Master File, such as instituting a brief delay on release of DMF data on individuals who can be claimed as dependents on tax returns.

We look forward to working with you to ensure public access to a vital source of information widely used to keep the public informed about issues we care about.
Thank you again for the opportunity to present these views.

Sincerely,

Rick Blum

Rick Blum
Coordinator

E-mail Comment to House Committee on Ways and Means Hearing on Social Security Death Records - February 2, 2012 from Stephanie Nordlinger (details at end).

February 14, 2012

The Death Master File and its Social Security Death Index have been extremely helpful to me as a California attorney handling probate and trust matters. I also use the SSDI regularly as an amateur genealogist. **The use of this index should not be restricted because its use for legitimate purposes far outweighs its use by criminals.**

I. Use By Lawyers in Probate Proceedings

In probate and estate planning, the free online DMF allows you to inexpensively prove that someone has died and locate current relatives who must be given notice of probate proceedings. My office is probating a 1964 Will where the first four beneficiaries are deceased. I didn't have to take my client's word for this, hire a genealogist or locate and pay for death certificates in a low value probate. I could give the court the date of death (at least the month and year) at essentially no cost for three of the four potential beneficiaries. The fourth wasn't in the SSDI because he had been a state government (UCLA) employee, but he was my client's father and my former client, so we could find his information easily.

Much more difficult in the same case were finding the names and addresses of the decedent's numerous first cousins and three children of his deceased first cousin. Due to divorces and remarriages many years ago, current family members didn't know all of the other relatives the court requires to be listed and notified of the filing of a petition for probate of a Will or the opening of an intestate estate. I used the DMF/SSDI with www.Switchboard.com, a genealogy program for record-keeping and some telephoning and e-mail to locate the children of the dead relatives of the deceased. The geographic information in the data (last residence and state where the Social Security number was issued) tells you which person of a given name is likely to be the person you are seeking. I was able to track down all except one of the relatives, and his sister said even she didn't know where he lived.

I did most of this work while the DMF/SSDI was online in the form it had been for years. Another question arose, and I went to it again but was referred to another U.S. Government website that said it was no longer publicly available. I went ballistic and gave a scathing review to the second website, although I admitted at the end of the survey that my real complaint was the unavailability of the SSDI.

Fortunately, I soon learned from another attorney that a version of the DMF was still available on the Church of Latter Day Saints' www.Familysearch.org website. So I did the research there. It is also available on www.Ancestry.com, which removes Social Security numbers for those dying in the last ten years. This may lead to errors when seeking people with common names. (An amateur genealogist has added my step-grandfather, John H. Wilson, to the wrong family tree.)

II. Other Legitimate Uses of the Death Master File

This was not the first, nor will it be the last, time I need the Social Security Death Index or the DMF for legitimate legal purposes. It has also been very helpful to me in doing:

(1) my own genealogy (since the 1980s),

(2) finding lost classmates for a reunion,

(3) cleaning out law office files (e.g., a file for a Will I drafted years ago) and

(4) cleaning up address books when you think someone has died or know they have but don't know the details. Or

(5) you may want to contact someone you have lost track of. You know their married name, and you can sometimes find the living person by finding the record of death of their spouse (or other relative).

III. A Free, Accessible Supplemental Index of State-Provided Death Records Would Also Be Helpful

I think the U.S. Government should also provide a free, public (Internet-accessible) Supplemental Index of the death information it has received from the states which often covers people who didn't have Social Security. I know some of it is wrong; I have seen death certificates where the decedent's name was misspelled and there were other errors. But it is much better than no index at all. **It is expensive to search state archives for a death certificate if you don't know the year of death or aren't sure of the place of death.**

For example, my maternal grandparents were divorced about 1915. My Mom visited her father in New Jersey in the late 1920s. She learned of his death several decades later, but she is deceased and I have no idea when or precisely where he died in the 1950s, 1960s or 1970s. It was probably in New Jersey, but it could have been in a hospital in New York or Philadelphia. He is not in the SSDI. When I asked the State of New Jersey to check certain years in a particular order and stop searching if it found his death record, its clerk returned my check and asked that I specify the years to be checked. They charge a fee for each year checked, and there's no point in checking after you find the record. If I had a date, this research would have been done a long time ago without spending more than $50 for a ten or fifteen dollar death certificate.

As an attorney, I previously represented a company that did delinquent credit card collections and we had access via a service called Accurint to records showing the people who had used the same Social Security number. Sometimes, there were quite a number of them. People will continue to use incorrect Social Security numbers for various reasons including the need to have a job without providing information on their previous criminal, immigration or other records, typographical errors, bad handwriting, avoiding judgments and ex-lovers, etc. While I know that one can lawfully request and get a new Social Security number, not everyone knows this. Credit agencies need to keep track of who is dead and who is alive, and the DMF helps them to do this.

IV. Conclusion

People will misuse Social Security numbers regardless of whether they have access to the DMF/SSDI. Depriving the rest of us of its legitimate uses will not prevent the abuse of

Social Security numbers. IRS's providing of taxpayer I.D. numbers to illegal immigrants has helped to reduce the number of intentional errors in the Social Security number database. We should keep the present free, Internet-accessible DMF/SSDI, add a new public index to state-provided death records and encourage people to correct their Social Security data with minimal or no penalties for the uninitiated who use other people's numbers to survive and not to defraud. Congress might even establish an amnesty period for making such corrections.

Sincerely yours,

Stephanie Nordlinger, Esq.
Law Offices of Stephanie Nordlinger
3933 S. Sycamore Avenue
Los Angeles CA 90008-1120.
(323) 299-3244
NordlingerEsq@aol.com

The Society of Thoracic Surgeons
Comments for the Public Record
House Committee on Ways and Means, Subcommittee on Social Security Hearing
The Accuracy and Uses of the Social Security Administration's Death Master File
February 2, 2012

The Society of Thoracic Surgeons (STS) is the largest organization representing cardiothoracic surgeons in the United States and the world. We are writing in response to the House Committee on Ways and Means – Subcommittee on Social Security hearing on "The Accuracy and Uses of the Social Security Administration's Death Master File."

Founded in 1964, STS is a not-for-profit organization representing more than 6,100 surgeons, researchers, and allied health care professionals who are dedicated to ensuring the best possible outcomes for surgeries of the heart, lung, and esophagus, as well as other surgical procedures within the chest. Thank you for considering these comments as you focus on this most important issue.

We are writing to express our concern and request your assistance with an issue of critical importance to our ongoing, cutting-edge, health care quality improvement efforts. As you are aware, beginning November 1, 2011, the Social Security Administration (SSA) rescinded its policy of sharing death reports that it receives from individual states. Reportedly, under the revised opinion of the SSA general counsel, SSA will only share state-originated death information with Federal agencies. This change in policy could compromise the ability of STS, and other medical specialties that utilize clinical registries, to successfully monitor long term patient outcomes. This information has been of vital importance to physicians and researchers who want to evaluate the success of medical interventions and who want to track other medical and public health related trends.

Linking clinical registries to the Social Security Death Master File (SSDMF) allows for the verification of "life status" of patients who otherwise would be lost for follow up after their treatment. Research based on this information helps physicians to advise today's patients and families and help them with decision-making. Outcomes data gives patients confidence in their medical interventions and demonstrates to patients and their families the durability and long-term benefits of medical procedures. These data also help medical societies when providing information to policymakers and regulators. For example, data can be used in research comparing the long-term effectiveness of alternative treatment strategies. It also has the potential to generate clinical and longitudinal comparative effectiveness research on a national level that can be evaluated based on patient demographics.

Utilizing these data, we have been able to link and follow patients who have had multiple operations in different institutions, perform long-term follow-up of repeat hospital admissions and additional procedures, and generate Kaplan-Meier survival curves. Physicians have also used these data to evaluate their respective outcomes against the national standard. Research of this sort is already the foundation of research on the safety and effectiveness of medical products and national payment and coverage decisions. (See attached for more information on the STS Database.)

As a medical society, STS has long advocated for the protection of patients' and our members' privacy. The STS Database upholds rigorous privacy protocols and is fully compliant with Health Insurance Portability and Accountability Act (HIPAA) requirements and Federal Common Rule protections for human subjects research.

We respect that Chairman Johnson has introduced H.R. 3475 in order to help to protect individuals' personal information. However, we request that the Congress restore access to all the data in the SSDMF for certain types of medical research that meets established privacy standards and exempt that research from the additional restrictions proposed under H.R. 3475. To that end, we have proposed the following change to the amendment to section 205(r) of the Social Security Act contained in H.R. 3475:

> Section 205(r) of the Social Security Act (42 U.S.C. 405) is amended--
> (1) in paragraph (5) by striking `for statistical and research activities' and all that follows and inserting `for law enforcement, tax administration, and statistical and research activities conducted by Federal agencies and for statistical and research activities conducted by State agencies, *as well as for other statistical and research activities conducted by medical, scientific, or public health researchers in accordance with the Federal Common Rule [46 C.F.R. § 46.101] and/or the applicable privacy and security rules issued under the Health Information Portability and Accountability Act of 1996 [45 C.F.R. Pt. 164 and § 512(i)], and subject to review and approval by an institutional review board registered with the Department of Health and Human Services Office of Human Subjects Protection and/or the Food and Drug Administration and accredited by the Association for the Accreditation of Human Subjects Research Protection Programs*.'; and

STS greatly appreciates the opportunity to offer these comments for the Committee's consideration. We look forward to working with you to achieve our mutual goal of protecting American's privacy and identities while ensuring that innovations in health care quality and technology are able to flourish. Please contact Phil Bongiorno, STS Director of Government Relations, at (202) 787-1221 or pbongiorno@sts.org if you have any questions.

Attachment

Background

In January 2008, in compliance with HIPAA, STS began to access the SSDMF in order to track long-term survival among cardiothoracic surgical patients. The SSDMF complements the STS Database by providing information about short-term and long-term survival. Linking STS Data to the SSDMF allows researchers to ascertain "life status" of patients who have undergone cardiothoracic surgical procedures.

About the STS Database

STS has long been at the forefront of efforts to improve healthcare quality. The STS National Database was established in 1989 as an initiative for quality improvement and patient safety among cardiothoracic surgeons. There are three components to the STS National Database, each focusing on a different area of cardiothoracic surgery—

- Adult Cardiac Surgery Database;
- General Thoracic Surgery Database; and
- Congenital Heart Surgery Database (Anesthesiology may also participate in the Congenital Heart Surgery Database).

The component databases provide participants with opportunities for quality improvement. The Society has developed quality performance measures in all three sub-specialties of surgery and these measures have either been endorsed or are in the process of being considered for endorsement by the National Quality Forum. By collecting outcomes data for submission to the STS National Database, surgeons are committing to improving the quality of care that their cardiothoracic surgery patients receive. The Database has the corollary potential to be a powerful tool for clinical research. Since its inception, more than 100 publications have been derived from Database outcomes. These studies have been published in a variety of professional journals and textbooks and have significantly advanced knowledge in cardiothoracic surgery.

The Database continues to expand with new initiatives. Launched in January 2011, STS Public Reporting Online enables Database participants to voluntarily report to the public their heart bypass surgery performance. Overall composite star ratings as well as their component ratings are listed on www.sts.org for more than 250 Database participants. The Adult Cardiac Surgery Database, now containing more than 4.5 million surgical records, represents an estimated 94 percent of all adult cardiac surgery centers across the U.S. With the success of participation nationally, in 2011 STS launched an initiative to accommodate Database participation worldwide by including international participants in the Adult Cardiac Surgery Database.

In general, the STS National Database provides:

- A standardized format for examining the care of patients undergoing cardiothoracic operations;
- A tool that can be used to target specific areas for clinical practice improvement;
- The ability to obtain an accurate reflection of practice patterns;
- The ability to research the national aggregate data set; and

- The opportunity to participate in a national quality improvement effort for thoracic surgery that has an impact at the local, regional, and national levels.

The Database offers a standardized format for examining the care of patients undergoing cardiothoracic surgical procedures which can be used to target specific areas for clinical practice improvement, obtain an accurate reflection of practice patterns, and conduct research using the national aggregate data set. Many third-party payers, major corporate purchasers of health care, hospitals, health care systems and states now require monitoring of outcomes and participation in quality improvement programs; participation in the Database fulfills these requirements.

STS envisions a health care system that reinforces meaningful quality improvement initiatives, including the acquisition and use of risk-adjusted reliable outcomes and clinical effectiveness data, and reward physicians for improved outcomes. Successful implementation relies on the integration of clinical and administrative data, allowing researchers to monitor the cost of care over time and provide an assessment of clinical and cost effectiveness, including issues related to new technologies and devices. However, only a clinical database with a sufficient volume of clinical records can be credibly risk-adjusted for case mix to yield accurate and comparable findings.

STS has successfully linked its clinical data with Centers for Medicare and Medicaid Services (CMS) MEDPAR information and the SSDMF to obtain longitudinal outcomes data for a wide array of cardiothoracic surgery operations. The ability to link clinical data with administrative data has opened up important new ways to assess the effectiveness of treatment options and offered new avenues for medical research. Clinical data yield sophisticated risk-adjustment assessments, while administrative data provide information on long-term outcomes such as mortality rate, readmission diagnoses, follow-up procedures, medication use, and costs. Linked data are also useful in conducting comparative effectiveness research.

TVT Registry

In addition, STS has recently undertaken to develop the National TVT Registry. The TVT Registry is the result of an ongoing collaboration between STS and The American College of Cardiology in support of Transcatheter Aortic Valve Replacement (TAVR) introduction in the United States. It was also developed in collaboration with the FDA and CMS, with input from The Society for Cardiovascular Angiography and Intervention (SCAI) and The American Association for Thoracic Surgery (AATS).

Approved by the FDA for use in the United States in November 2011, TAVR technology is now an option for elderly patients with aortic stenosis who are too sick, frail, or high risk for conventional surgical therapy. The TVT Registry will capture and house patient demographics, procedure details, and facility and physician information. This standardized, evidence based data source will offer much insight into clinical practice patterns and patient outcomes. The TVT Registry serves as the main repository for all clinical data related to TAVR and is positioned to incorporate additional catheter-based procedures that have yet to come to market in the United States. The TVT Registry was designed to be linked to the SSDMF and CMS databases in order to track long term outcomes. Physician participation in such a clinical registry was a condition of FDA approval of the Edwards Lifesciences SAPIEN device and is expected to be a condition for Medicare reimbursement for TAVR procedures.

Susan L. Lubow
5 Easley Terrace
Morristown, NJ 07960
973-267-2784
holijoli@aol.com

To: Congressman Dave Camp
House of Representatives Committee on Ways and Means

Re: Hearing on Social Security Death Records (use and impacts of the death masterfile)

As an amateur genealogist who has been doing this work for forty years, I would like to emphasize the importance of the public availability of this record in digitized form. Most particularly, for people like me, it is important to keep this record on the internet.

The actual social security number should **not** be available and never should have been put on-line. A person's name, date and place of birth, and date and place of death/receipt of benefits are vital information for people researching family history or looking for family members. These activities have become very important to many people throughout our country.

I cannot believe that privatizing this information will make much of a difference to anyone who is intent on wrongdoing, but it will throw up enormous obstacles to those of us who are honestly seeking information for no personal gain.

I hope that you will consider merely removing the social security numbers from the data available to the public, but letting the rest of the information continue to be accessed.

Thank you for your consideration.

Tel: 973-267-2784 Fax: 973-267-4513 email: holijoli@aol.com

I submit this request to keep Open the masterfile for the Social Security Death Records.

Genealogists worldwide use these records for personal and business reasons -- for genealogical search.

Eliminating access is an elimination of Freedom of Information for all people. We cannot allow our rights to information to be chipped away ... bit by bit.

Name: Susan Williams

Phone # 732-606-6086

E-mail: swilliams1200@comcast.net

Title of Hearing -- Social Security Death Records

Susan Williams

Floyd Martin
Texas City Ancestry Searchers
2814 Lynn Circle
Texas City Texas 77590
zingo1226@yahoo.com
Type of hearing - removing the Social Security Death Index

Sirs:
Birth and death have long been a matter of public record. The social security death index is virtually the only tool we have to determine birth and death dates in many areas. Removing this service from the public is not only complete ridiculous but a violations of our rights without a valid reason. This is not where with privacy pirates get their information anyway. These records are for the deceased and not the living.

I do an awful lot of indexing of records so the public can research their family histories. I was the 2008 Texas State Genealogy Societies volunteer of the year. I digitize records for the public every day. I have digitized many thousands of documents I have digitized over 97,000 for family search.org. alone

There is absolutely no just cause for the attempt of this action and is an infringement of our rights. There is nothing illegal about our use of the Social Security Death index. This is merely a misguided attempt by those in power who have no real idea what they are talking about that are attempting to take unnecessary and in our opinion a violation of the freedom of information laws.

February 3, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Terese Vekteris
6125 McCallum Street
Philadelphia, Pa 19144

Friday, February 03, 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

Currently, four bills are pending in the US Congress that would eliminate or curtail access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* http://tinyurl.com/6uwu4aw
(If enacted, this bill would effectively end public access to the death file)
- S 1534, the Identity Theft and Tax Fraud Prevention Act http://tinyurl.com/75de8o9
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3482, To prevent identity theft and tax crimes. http://tinyurl.com/83p4b4p
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)
- HR 3215, To prevent identity theft and tax fraud http://tinyurl.com/7fgsd5s
(If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, the violations occur due to computer breaches from government and private enterprises. In fact, SSDI is actually a deterrent to identity theft. As posted on the National Technical Information Service (NTIS) website (**http://tinyurl.com/yb6e49e**), it states, that the Death Master File (SSDI is the commercial name of this list) prevents identity fraud, as it verifies a person's death. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others.

Genealogists doing US research located both in and outside the United States rely heavily on the SSDI. The Death Master File is a computer database file that has been made available by the United States Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

Tina Daggett
1215 Barry Ave Apt 5
Los Angeles, CA 90025

Virginia Genealogical Society
1900 Byrd Avenue, Suite 104
Richmond, Virginia 23230-3033

February 15, 2012

U.S. House Ways and Means Committee
Committee Office
1102 Longworth House Office Building
Washington, DC 20515

Re: Social Security Administration's
Death Master File: 2/2/2012 hearing

Dear Sirs:

On behalf of the Virginia Genealogical Society ("VGS"), a Virginia nonprofit corporation which recently celebrated its 50th anniversary and which has over 1600 members, with its address at 1900 Byrd Avenue, Suite 104, Richmond, Virginia 23230, I would like to submit this statement for the record in the above hearing. I am a director and former President of VGS, as well as its legal counsel.

VGS believes that any effort to limit or block public access to decedents' social security numbers, which are currently publicly available through the Social Security Administration's Death Master File, is misguided.

As background, a decedent's social security number use dies with the decedent; the decedent's estate must obtain its own federal tax identification number.

Public availability of the Death Master File is not only very helpful as a genealogical and historical research tool to pinpoint date of death, date of birth, and last residence of a decedent, but is important for other reasons as well.

It is also a valuable tool used in tracking down living heirs. It is not uncommon in rural Virginia to have a parcel of family-owned real property with the deed in the name of an ancestor who died in the 19th or early 20th centuries. To sell the property and track down out-of-state heirs, the social security death index often provides a critical tool to confirm the death of an out-of-state heir, and to use the last place of residence of that decedent to track down living heirs of the next generation in that same geographical area.

It is also important to have public access to the Death Master File to prevent identity theft. It is often necessary to widely distribute death certificates (which generally contain social security numbers) in the course of settling estates and collecting and distributing assets. Depending on the type of assets which a decedent owns, parties holding death certificates may

include the funeral home, the monument company, the cemetery, financial institutions, insurance companies, clerk's office (to open a probate file) and real estate clerk's or recorder's office (to record transfers of real property held by the decedent). Records held in local clerk's offices (including death certificates) are normally public records in most states. If the decedent held assets in foreign countries, it is often necessary to record the U.S. death certificate (with social security numbers) in public records in the foreign countries to transfer assets.

At present, the necessary and widespread distribution of death certificates (with social security numbers) poses little risk of identity or credit theft because of the public availability of the Social Security Death Master File. This low risk occurs because lenders routinely check the Social Security Death Master File, to make sure that no new credit cards or other credit extensions are being made under a decedent's social security numbers. Since the decedent's estate has its own taxpayer identification number, the credit and personal information under the decedent's social security number should show no new activity following death. A request for new credit using a decedent's social security number is such an easy and obvious crime to detect that it rarely occurs once the name is published in the Death Master File.

If public access to the Social Security Death Master File were cut off, since death certificates with social security numbers are often widely distributed (as described above), there would be no way for lenders to know of a death, and they could be duped into significant credit extensions to a criminal claiming to be the decedent, with a changed address. It can reasonably be expected that criminals would quickly seek to exploit this new opportunity, relying upon a decedent's good credit to establish fraudulent new accounts under the decedent's social security number (which could be obtained from any of the sources noted above). Massive fraud losses could reasonably be expected.

On the other hand, the fraud claims under the current public disclosure system are relatively limited, apparently primarily limited to taxpayers falsely claiming deceased children of other persons as dependents on an income or other tax return. This should be a "stupid" crime, with the IRS and Social Security promptly and aggressively prosecuting the criminals, who should have no defenses to such a false claim and identity theft.

Instead, because the IRS and/or Social Security are failing to promptly prosecute thieves, this bureaucratic inaction is understandingly causing emotional harm to the decedent's relatives once they learn that someone is misusing the social security number of their deceased child.

This current abuse of the system by criminals is reprehensible, but fortunately is occurring on a relatively small scale. The solution is not to shut down the Death Master File, but to i) vigorously prosecute the criminals falsely claiming deceased children as dependents (these criminals should be easy to find and convict through their signed tax returns), and ii) consider creating a private cause of action for civil claims by the decedent's relatives, with substantial statutory damages similar to statutory copyright damages, plus attorney's fees, which could provide decedent's relatives with a substantial measure of satisfaction in seeking this relief against the criminals and obtaining substantial judgments against them.

VGS urges the Committee to take a rational approach to address a fairly limited number of fraudulent claims, rather than penalize genealogists, historians and persons searching for heirs who use the database. Please do not close what are now public records for no valid reason, and potentially open the floodgates to widespread fraud which would be extremely difficult to prevent or uncover.

Sincerely,

/s/Peter E. Broadbent, Jr.

#1244946

U.S. House Ways and Means Committee

Re: Social Security Administration's Death Master File
2/2/2012 Hearing

WITNESS SUBMISSION INFORMATION

1. Organization on whose behalf the witness appears: VIRGINIA GENEALOGICAL SOCIETY

2. Witness name: Peter E. Broadbent, Jr.

3. Witness business and contact information:

Christian & Barton, LLP
909 E. Main Street, Suite 1200
Richmond, VA 23219
Tel: 804-697-4109
Fax: 804-697-6109

4 February 2012

House Ways and Means Committee
Subcommittee on Social Security
B 317 Rayburn House Office Building
Washington, DC 20515

Subject: OPPOSE HR 3475, S 1534, HR 3482, AND HR 3215

Genealogists support Congress's intent to protect Americans from improper usage of their personal information, and to protect them from identity theft. However, genealogists DO NOT support restricting access to public records that have very little to due with identity theft.

The Death Master File is a computer database file made available by the United States Social Security Administration since 1980. It is known commercially as the Social Security Death Index (SSDI). The Death Master File is considered a public document under the Freedom of Information Act.

Currently, four bills are pending in the US Congress that would eliminate or curtail public access to the Social Security Death Index (SSDI) on the Internet. I oppose all of these bills, which are:

- HR 3475, *Keeping IDs Safe Act of 2011* (http://tinyurl.com/6uwu4aw - If enacted, this bill would effectively end public access to the death file.)
- S 1534, *Identity Theft and Tax Fraud Prevention Act* (http://tinyurl.com/75de8o9 - If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death.)
- HR 3482, *Tax Crimes and Identity Theft Prevention Act* (http://tinyurl.com/83p4b4p - If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death.)
- HR 3215, *To prevent identity theft and tax fraud* (http://tinyurl.com/7fgsd5s - If enacted, this bill prohibits disclosure of the deceased's SSN in calendar year of death and calendar year following death.)

Rarely has it been documented that an individual's identity is violated by access to SSDI; rather, such violations occur due to computer breaches of government and private enterprises. In fact, access to the SSDI is actually a deterrent to identity theft. According to the National Technical Information Service's website (**http://www.ntis.gov/products/ssa-dmf.aspx**), access to the Death Master File helps the financial community, insurance companies, security firms and state and local governments comply with the Patriot Act by identifying and preventing identity fraud. The SSDI is used by credit reporting agencies, merchants, private investigators looking for missing heirs in probates, media reporters, university researchers, and others. It is used by financial and credit firms and government agencies to match records and prevent identity fraud.

Genealogists located both in and outside the United States doing US research rely heavily on the SSDI, which has been made available by the US Social Security Administration since 1980.

I oppose HR 3475, S 1534, HR 3482, and HR 3215.

Thank you,

William W. Josey
4410 Franklin Street
Kensington, MD 20895

○