U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Protecting the Privacy of the Social Security Number from Identity Theft

The Honorable Patrick P. O'Carroll, Jr.

Inspector General, Social Security Administration

June 21, 2007

Good morning, Chairman McNulty, Mr. Johnson, and members of the Subcommittee. Thank you for the invitation to be here today to discuss the Social Security number (SSN) and how we can better protect it and the American people.

The Office of the Inspector General (OIG) at the Social Security Administration (SSA) came into being in 1995, with the implementation of the Social Security Independence and Program Improvements Act of 1994. As a new entity charged with preventing and detecting fraud, waste, and abuse in SSA's programs and operations, we were well aware of the central role that the SSN played in American society, and the critical need for us to protect its integrity. With SSA, we have made significant strides towards that end since our early days. However, we are keenly aware that much more needs to be done. Today, I will provide you a brief history of our audit and investigative efforts, which have played an important role in strengthening SSN integrity - especially in the way these important numbers are assigned. But, more importantly, I will provide you with perspective on areas in which action is still needed-perhaps through additional legislation-to better protect SSNs from unnecessary collection and improper disclosure. I believe the American people expect and deserve our attention to address this vital matter.

Well before 9/11, and even before identity theft became as significant an issue as it is today, we knew we had much work to do to strengthen SSN integrity. We were especially aware of the broad uses of SSNs throughout U.S. society and their importance to noncitizens while they are in the U.S. We also recognized that SSNs are the cornerstone of SSA's programs and, therefore, before we could turn too much of our attention outward-to the use and misuse of SSNs-we first needed to make sure that everything was in order within SSA. As a result, much of our early SSN work was in the area of enumeration-the process by which SSA assigns SSNs. If SSA's enumeration processes were not sound, no amount of improvement to the use and security of the SSN after it was issued would be of much value.

Since 1999, when we issued a Management Advisory Report emphasizing the importance of proper SSN assignment and use, we have worked closely with SSA to improve controls in the enumeration process. Based on our recommendations, collaborative efforts and new legislative requirements, SSA has improved the enumeration at birth and enumeration at entry programs, heightened the awareness of SSA employees to fraudulent identification documents presented with applications for SSNs, tightened controls over the issuance of replacement Social Security

cards, and otherwise made it much more difficult to obtain a valid SSN through the use of a fraudulent application.

During this period, my predecessors testified before this Subcommittee and other Committees and Subcommittees of both houses of Congress on SSN-related issues many times, presenting the results of our work, responding to requests from Members, proposing legislation, and seeking ways to further improve SSN integrity.

The September 11 attacks underscored the need to continue those efforts, but with respect to SSNs, did not teach us anything we did not already know about the critical role of the SSN in our society. In the months following 9/11, we worked with the FBI and other law enforcement agencies to provide critical information, and began a series of SSN-based Homeland Security initiatives. These projects sought to ensure, through review of SSNs and other information, that individuals with access to critical infrastructure sites such as airports, seaports, nuclear power plants, and similar locations, were who they claimed to be, and not imposters who would do us harm.

Even while working on Homeland Security matters, our investigators continued their day-to-day work on individual SSN misuse cases, bringing to justice scam artists, identity thieves, counterfeit document artists, and other criminals whose tool of the trade was the purloined SSN. On an annual basis, we receive about 10,000 allegations of SSN misuse a year, and investigate approximately 1,500 criminal cases of misuse. After years of increases, these numbers have now held steady for several years, indicating that not only our investigative work, but also our audit work, is having a significant impact.

Having completed numerous audits that helped SSA strengthen its enumeration processes, in more recent years our auditors have begun to address the far more challenging issue of SSN misuse. While SSA can implement controls to prevent the improper assignment of SSNs, it has very few mechanisms to curb the improper-or simply the unnecessary-use of an SSN. Our audit and investigative experiences have taught us that the more SSNs are used unnecessarily, the higher the probability that these numbers could be improperly disclosed and used to commit crimes throughout society. We read about these occurrences in the newspaper every day, but we've yet to develop meaningful ways to stem the tide.

As I'll discuss in a moment, our recent audit work has highlighted vulnerabilities and suggested some ways in which SSA can try to persuade organizations that use SSNs to limit this use and better protect this sensitive information. To some extent, these efforts, along with the users' own experiences with improper disclosures, have convinced some organizations to do as we and SSA have suggested. However, because it is such a convenient and unique number, and change may be costly, others appear to discount the risk and continue on with business as usual. To convince these parties, we believe SSA needs more help. Specifically, we believe the time has come to consider legislation limiting the collection and use of SSNs to those purposes mandated by Federal law, or otherwise reducing the use of SSNs as convenient identifiers.

In 2002, the Federal inspector general community joined with us to look more closely at one high-risk issue regarding SSNs: agencies' controls over access, disclosure, and use of SSNs by external entities, such as contractors, within their respective agencies. A total of 15 Offices of

Inspector General participated in this effort, each conducting an audit within their respective Agencies. We combined our results and provided a comprehensive report, which included recommendations to improve the security of the SSN at the Federal Government level. While we believe that our work, and the work of our fellow inspectors general, brought about improvements in SSN security and heightened awareness of the issue, there is more to be done. Recent OMB guidance makes it clear that at least at the Federal level, uses of the SSN must be curtailed, and security measures enhanced. We will continue to monitor the Federal sector's progress in accomplishing this mandate.

Of course, the Federal Government is not the only source of SSN information. As I'm sure you're aware, schools, businesses, and State and local governments request SSNs for a multitude of purposes-very few of which are required by law. Rather, many of these organizations use the SSN as an identifier simply because it is convenient. For example, our auditors have looked at the use of SSNs by universities and hospitals as student and patient identifiers, respectively. While both of these types of organizations may have had some reason for collecting SSNs, such as financial aid or Medicare coverage, we found that once collected, the number was used too frequently for other purposes and not always given the level of protection necessary.

In response to our audits, SSA outreach, and their own experiences with data exposures, many universities are moving away from using SSNs as student identifiers. However, in an audit currently underway, we were disturbed to learn that 43 States collect the SSNs of students in kindergarten through 12th (K-12) grade. In only three of these States is the collection of these numbers required by law. The No Child Left Behind Act of 2001 requires that each State implement an accountability program that measures the progress of students and schools through the collection and analysis of data. However, the law does not require that States use SSNs to identify and track students. Rather, we believe that some K-12 schools use SSNs as a matter of convenience. For example, while we did not perform a statistical sample, we know of some schools and districts that still print the students' SSNs on attendance rosters. We would suggest that the security of individuals' personal information-in this instance, the personal information of children-not take a back seat to administrative convenience. For the 2004/2005 school year, the National Education Association estimated that there were more than 48 million K-12 students in over 15,000 school districts across the country. We believe that the collection and use of SSNs without proper controls is a huge vulnerability for this young population. Recent data indicate the number of children under age 18 whose identities have been stolen is growing. This is particularly troubling given that some of these individuals may not become aware of such activity until they apply for a credit card or student loan.

We also found that State and local governments use the SSN as an identifier for other programs, such as prescription drug monitoring, when other identifiers such as drivers license numbers might be more appropriate. Additionally, these entities don't always provide sufficient protection of this data.

We even conducted an audit that looked at the access prisoners are sometimes given to SSNs while doing work in prison on State records or other documents containing SSNs and other personal information. The possibility of giving a convicted identity thief access to the tools of his or her trade while in prison is certainly alarming.

I'm proud of the work that has been done, and continues to be done, by both our Office of Audit and our Office of Investigations, but our focus on SSN integrity does not stop there. Several years ago, in order to keep track of our many-faceted effort to protect the SSN, we formed the Social Security Number Integrity Protection Team, or SSNIPT. That group, comprised of attorneys, auditors, and investigators, has had its own quiet-but important-successes. It was in part the efforts of the SSNIPT team that led to the eradication of the display of SSNs on Selective Service mailings and the Thrift Savings Plan website-two practices in which the Federal government was itself putting the SSN at risk. The team has also worked to propose legislation, which was ultimately enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), to eliminate the practice of displaying SSNs on drivers licenses. All of our exhortations over the years aimed at getting Americans to stop carrying their Social Security cards in their wallets would be of little value if the one document they were required to carry also displayed their SSN.

The OIG will not waver in our commitment to protect the integrity of the Social Security number through our timely audit, investigative, and other work, and we welcome Congress' help. Legislation has been, and will always be, a key factor in our ability to protect the SSN and protect the American people. Legislation has, to some degree, improved enforcement mechanisms in this area (the Identity Theft Penalty Enhancement Act), but legislation that would limit the display of SSNs on public documents or eliminate the sale of SSNs by information brokers has not yet been passed, with the exception of the IRTPA provision concerning drivers' licenses. Similarly, no law has been passed to address the unnecessary collection of SSNs by schools, hospitals, or other entities that use this number as a matter of convenience but fail to adequately protect this personal information.

There are, however, a number of bills that have been introduced. In the last Congress, H.R. 1745, as well as the current Congress' S. 238, each seek to address both the display and the sale of SSNs, and H.R. 948, while silent on the display of SSNs, would also prohibit their sale under many circumstances. Any legislative provisions that reduce the display of SSNs or limit or eliminate trafficking in SSNs by information brokers and others would be of great help to our efforts.

It is important, however, not only to stop intentional criminal behavior, but to place an onus on those who use the SSN-either because they are required to do so by law, or because the SSN is a convenient identifier-to protect the information they are holding.

Consider an investigation we recently concluded in which several people were convicted of SSN misuse on a large scale. The primary subject of the investigation was a manufacturer of fraudulent identification documents that he created using real names and SSNs that his co-conspirators obtained. The documents were then used to defraud banks, businesses, and individuals out of more than half a million dollars. The names, SSNs, and other data were stolen from banks and from a hospital where security measures were obviously inadequate to prevent or detect the theft.

This individual and his co-conspirators are being criminally prosecuted, but criminal prosecution is not always an option. One proposal we have made in the past is that the OIG's Civil Monetary Penalty authority be extended to include SSN misuse. Providing the authority to penalize those

who misuse SSNs but are not criminally prosecuted, or to penalize institutions that collect, but fail to protect, SSNs could create a strong deterrent and an effective tool.

The OIG has proven its ability to administer such a program through its administration of the existing provisions of Sections 1129 and 1140 of the Social Security Act-and we are prepared to take on this new challenge.

Indeed, we are faced with new challenges on a daily basis, as we constantly find new ways to close gaps in the SSN's protection. We are currently examining the practice of assigning SSNs to noncitizens who will only be in the United States for a few months-but are allowed to obtain an SSN that will be good forever. Consider, for example, the practice of allowing noncitizens who enter the country with a fiancé visa to obtain an SSN. While deciding whether they will marry, these noncitizens are allowed to stay in the United States for 3 months-after which time they must marry, leave the country or apply for a new immigration status with DHS. By approving their request for an SSN during this 3-month period, we might be giving those who have no intentions to marry a much-needed tool for overstaying their visas. We believe a wiser course of action would be to approve the SSN application after the marriage has occurred, but we may need a legislative remedy to implement such a policy. Additional opportunities exist to restrict SSN access to other populations that might take advantage of similar programs.

We've also just undertaken an audit concerning the display of the SSN on Medicare cards, a document that many Americans carry in their wallets. I mentioned earlier our attempts to remove the SSN from drivers' licenses; while the use of the SSN in the Medicare program may be necessary, the display of the SSN on the card is something we'll be taking a critical look at.

As we have stated before this Subcommittee on many occasions, the SSN was never intended to do more than track a worker's earnings and pay that worker benefits. As the uses of the SSN have expanded over the decades, through acts of Congress and through the SSN's adoption simply as a matter of convenience, its value has increased as a tool for criminals. The Social Security card itself, which states on its face that it is not to be used for identification, is frequently cited as needing improvement. But spending billions of dollars to try and stay one step ahead of counterfeiters is not the answer. The answer lies in doing everything we can to ensure the integrity of the enumeration process; limit the collection, use, and public display of the SSN; encourage the protection of the SSN by those who use it legitimately; and provide meaningful sanctions for those who fail to protect it or who misuse it themselves.

We will continue our audit work in these areas, such as the fiancé visa audit I just mentioned. We will continue our investigations, such as those I've described today. We will continue working to ensure Homeland Security, as reflected in the role we played in the recent arrests of terrorists planning an attack on Fort Dix. We will continue to seek the prosecution of employers or others who knowingly provide false SSNs to employees otherwise not authorized to work in the United States, as we did just last week in the Pacific Northwest, where a staffing agency was allegedly providing illegal workers with fraudulent SSNs. And we will continue to work with SSA and with this Subcommittee in hearings such as this, and in seeking legislation to make our efforts still more effective.

Thank you, and I'd be happy to answer any questions.