DISCLAIMER

Electronic versions of the exhibits in these minutes may not be complete.

This information is supplied as an informational service only and should not be relied upon as an official record.

Original exhibits are on file at the Legislative Counsel Bureau Research Library in Carson City.

Contact the Library at (775) 684-6827 or library@lcb.state.nv.us.

Statement of Honorable John G. Huse, Jr., Inspector General, Social Security Administration

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

Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers

May 22, 2001

Good morning, Mr. Chairman, Congressman Matsui, and members of the Subcommittee. As you know, my office is charged with protecting Social Security programs from fraud, waste, and abuse. No aspect of our mission is more important than our oversight of the use--and misuse--of the Social Security account number, or SSN.

In 1935 the SSN was created as part of a new system to track the earnings of employed Americans. Just as no one dreamt that the innocuous nine-digit number would become our *de facto* national identifier, no one could foresee the breadth and complexity of commerce in an electronic age. But by 1967, when the Department of Defense abandoned the military identification number in favor of the SSN for armed forces personnel, the theories that would eventually give rise to today's Internet were already being debated. In the quarter century since, the myriad uses of the SSN have continued to expand, while the notion of a worldwide network of computers evolved from theory to reality. Unfortunately, while the SSN and computer technology have matured together, the laws we use to police and protect them have struggled to keep pace.

Misuse of the SSN, catalyzed by the Internet, has quickly become a national crisis. The SSN's universality has become its own worst enemy. The power it wields--power to engage in financial transactions, power to obtain personal information, power to create or commandeer identities--makes it a valuable asset and one that is subject to limitless abuse. It falls on Government, which created the SSN and permitted it to assume such power, to take action to control its own creation. Organizations such as the Social Security Administration, its Office of the Inspector General, the Federal Trade Commission, and the Department of Justice have the responsibility to enforce laws designed to protect against SSN misuse and its consequences. To do so, there must be adequate laws in place.

In recent years, we have seen the enactment of The Identity Theft and Assumption Deterrence Act of 1998 and the Internet False Identification Prevention Act of 2000. The former is the first legislative response to the growing wave of identity thefts and imposes criminal sanctions for those who create a false identity or misappropriate someone else's. The latter closed a loophole left by the first, enabling my office and other law enforcement organizations to pursue those who previously could sell counterfeit Social Security cards legally, by maintaining the fiction that such cards are "novelties," rather than counterfeit documents. Both pieces of legislation are helpful, but both treat the Identity Theft disease in its latest stages, rather than at onset. Identity Theft begins, in most cases, with the misuse of an SSN, and while the ability to punish Identity Theft is important, the ability to *prevent* it is even more critical.

How do we do this? First and foremost, the time has come to put the SSN back into its box. We as a Government created the SSN, and we as a Government must control it. We must make the difficult determinations as to those uses that are appropriate and necessary, and those that are merely convenient. The SSN is a unique identifier, and its quotidian use as an I.D. number by schools,

hospitals, and other institutions is understandable--but dangerous. Its use by Federal, State, and local governments not only for taxes and other legitimate purposes, but for everything from drivers' licenses to water and sewer bills, is a convenience that we can no longer afford. Its use in private industry, not just for financial transactions, but for joining a health club or buying a refrigerator, has become reckless. And its ready availability over the Internet must come to a stop.

We need legislation that limits the use of the SSN to those purposes that benefit the *holder* of the SSN, not the company that sells that person an appliances or the state that issues that person a drivers' license--legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. I am sensitive to the costs that would be incurred in both the public and the private sectors in implementing the changes that such legislation would require, and I do not suggest that any of us are facing an easy task. Rather, it is a necessary task. The appropriate agencies, in cooperation with governmental authorities and business leaders, must reach an understanding as to the need to limit the use of the SSN and regulations would have to be promulgated reflecting such uses and providing for enforcement mechanisms. In addition, the legislation would need to outlaw the sale of SSNs over the Internet and through other means. With certain legislated exceptions, no private citizen, no business interest, and no ministerial government agency should be able to sell, display, purchase, or obtain any individual's SSN, nor should they be able to use any individual's SSN to obtain other personal information about the individual.

The prevalence of SSN misuse cannot be denied. In Fiscal Year 2000, our office received 92,847 allegations. Over half of them, 46,840, were allegations of SSN misuse, and another 43,456 were allegations of program fraud, which experience has shown us often include implications of SSN misuse. My office and others, such as the FTC, are doing all we can within the limitations imposed by existing law and resources. We are diligent in referring allegations of Identity Theft to the FTC, and we conduct investigations of SSN misuse, both program-related and non-program-related, on a daily basis. We have conducted undercover operations in which we have purchased counterfeit Social Security cards, and reverse-sting operations in which we have offered such cards for sale. Several of these cases are now pending in U.S. Attorney's Offices. We are involved now in a joint investigation with another Federal law enforcement agency in which lists of names and SSNs were being sold to the highest bidder on an Internet auction site. Although the investigation is ongoing, and I cannot provide details, I can tell you that we've discovered that the source of the lists was a university. This highlights the need to stop the indiscriminate use of SSNs as I.D. numbers. Unfortunately, while the subject in this case may eventually face criminal charges of some kind, nothing in the Social Security Act currently prohibits the sale of SSN information.

In addition to legislation that limits the use of SSNs and provides sanctions for violations, and legislation which criminalizes the sale and purchase of SSN information, it is important to provide an administrative safety net, as well. Our Civil Monetary Penalty program has proven an invaluable asset in the context of SSA program violations when criminal prosecution is not a viable option. Similar authority in the arena of SSN misuse would provide my office with the same ability to take administrative action. I would urge you to consider legislation vesting in us such authority.

With legislation such as that I have discussed, and the continuing dedication of the Government agencies involved, and of this Subcommittee, I am confident that we can reverse the trend of SSN misuse and Identity Theft.

I welcome this Subcommittee's dedication and attention to this critical issue, and I would be happy to answer any questions.