INTEGRITY OF GOVERNMENT DOCUMENTS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT
REFORM AND OVERSIGHT
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

MARCH 7, 1995

Printed for the use of the Committee on Government Reform and Oversight

U.S. GOVERNMENT PRINTING OFFICE
20–679 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052020-7

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

WILLIAM F. CLINGER, JR., Pennsylvania, *Chairman*

BENJAMIN A. GILMAN, New York
DAN BURTON, Indiana
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
STEVEN SCHIFF, New Mexico
ILEANA ROS-LEHTINEN, Florida
WILLIAM H. ZELIFF, JR., New Hampshire
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
PETER BLUTE, Massachusetts
THOMAS M. DAVIS, Virginia
DAVID M. McINTOSH, Indiana
JON D. FOX, Pennsylvania
RANDY TATE, Washington
DICK CHRYSLER, Michigan
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
WILLIAM J. MARTINI, New Jersey
JOE SCARBOROUGH, Florida
JOHN B. SHADEGG, Arizona
MICHAEL PATRICK FLANAGAN, Illinois
CHARLES F. BASS, New Hampshire
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
ROBERT L. EHRLICH, JR., Maryland

CARDISS COLLINS, Illinois
HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, JR., South Carolina
LOUISE McINTOSH SLAUGHTER, New York
PAUL E. KANJORSKI, Pennsylvania
GARY A. CONDIT, California
COLLIN C. PETERSON, Minnesota
KAREN L. THURMAN, Florida
CAROLYN B. MALONEY, New York
THOMAS M. BARRETT, Wisconsin
GENE TAYLOR, Mississippi
BARBARA-ROSE COLLINS, Michigan
ELEANOR HOLMES NORTON, District of Columbia
JAMES P. MORAN, Virginia
GENE GREEN, Texas
CARRIE P. MEEK, Florida
FRANK MASCARA, Pennsylvania
CHAKA FATTAH, Pennsylvania

BERNARD SANDERS, Vermont (Independent)

JAMES L. CLARKE, *Staff Director*
KEVIN SABO, *General Counsel*
JUDITH McCOY, *Chief Clerk*
BUD MYERS, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

MICHAEL PATRICK FLANAGAN, Illinois
PETER BLUTE, Massachusetts
THOMAS M. DAVIS, Virginia
JON D. FOX, Pennsylvania
RANDY TATE, Washington
JOE SCARBOROUGH, Florida
CHARLES F. BASS, New Hampshire

CAROLYN B. MALONEY, New York
MAJOR R. OWENS, New York
FRANK MASCARA, Pennsylvania
ROBERT E. WISE, JR., West Virginia
JOHN M. SPRATT, JR., South Carolina
PAUL E. KANJORSKI, Pennsylvania

EX OFFICIO

WILLIAM F. CLINGER, JR., Pennsylvania
CARDISS COLLINS, Illinois

J. RUSSELL GEORGE, *Staff Director*
TONY POLZAK, *Professional Staff Member*
ANDREW G. RICHARDSON, *Clerk*
MATT PINKUS, *Minority Professional Staff*
DAVE McMILLEN, *Minority Professional Staff*

CONTENTS

Statement of:

Letters, statements, etc., submitted for the record by:

INTEGRITY OF GOVERNMENT DOCUMENTS

TUESDAY, MARCH 7, 1995

U.S. House of Representatives,
Subcommittee on Government Management,
Information, and Technology,
Committee on Government Reform and Oversight,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:15 p.m., in room 2154, Rayburn House Office Building, the Honorable Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Flanagan, Davis, Bass, and Maloney.

Staff present: J. Russell George, staff director; Tony Polzak, professional staff member; Andrew G. Richardson, clerk; Matt Pinkus, Dave McMillen, minority professional staff members.

Mr. Horn. A quorum being present, the hearing will begin.

Our first guest on the first panel is a distinguished Member of Congress from southern California, Representative Xavier Becerra.

Representative Becerra.

STATEMENT OF HON. XAVIER BECERRA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Becerra. Thank you, Mr. Chairman.

Thank you to Mrs. Maloney and the members of the committee for the generous opportunity to come before you to talk a little bit about something that I believe is getting a great deal of attention these days, and that is, of course, the whole issue of tamper-proof identification cards, counterfeiting; what we can do to try to make sure that any document for identification purposes which the Government issues, or perhaps anyone in the public or private sector, issues, that we ensure that that card is used for the purpose that it was first issued.

In the process of providing some testimony here, let me try to focus on the three salient points that I think must be addressed by any body that is considering the whole issue of tamper-proof identification cards.

First, I think you have to take a look closely at the system and the data that is used for the purpose of developing a tamper-proof identification card. Is the data base clean? Is it accurate?

Second, I think you need to take a look at the whole issue of the risks posed by going toward some form of identification card which may be used to identify the general public and the concerns with privacy that may be involved there.

Finally, I would like to also touch on the whole issue of cost: Can we do it? How much will it cost?

Turning to the first point of accuracy of data, I hope that, in listening to some of the eloquent testimony you will have from the witnesses who will come before you today, you have a chance to ask some questions about things like what we have right now in the private sector that allows us to have identification cards or numbers.

I know that there have been some proposals that perhaps the Government should go the route of the private sector and get to the point where we have cards that are similar to ATM machine cards, where you can use a PIN code and have access to information.

I would only point out that we've had some work done on that, some studies done on that that show that error rates can be as high as 46 percent in some cases. That was as a result of a study done in 1991, which showed that two companies by the names of Citicorp and TRW, not unfamiliar names to us, had a survey done on their work in data matches that they had performed.

It was found that they had 46 percent and 28 percent error rates based on incorrect data. And that's from testimony that was gleaned from a 1991 hearing before the Subcommittee on Social Security before the Ways and Means Committee.

We also know that there are many systems. INS, for example, is operating under a system that is somewhat outdated. They are trying to perfect the system, update it, but obviously it does cost money and does take time. In order for these different systems, whether it's internally within an agency or between agencies, to communicate with each other, they must be able to have data that can correlate to each particular agency's data base.

I know that there has been other evidence presented. Back in 1993, for example, in October, in a Banking Committee hearing, it was revealed that over 1 million consumers use credit correction or credit restoration services. Obviously, they do that because what they find is that the credit information that is listed for them is inaccurate. So we find that there is a need to make sure that, whatever we do, we ultimately start off with good, solid, accurate data.

Let me move to the issue of privacy implications and access issues within any type of national ID system or a registry system. We first must take into account the current laws that we have that protect privacy. We have the Privacy Act of 1974; we have the Computer Security Act of 1987, both, along with other laws, are there to ensure against unauthorized use of information.

We have found in the past, through studies by the GAO or the Department of Justice, that there are serious problems with the quality and the availability of this data. According to the Immigration Reform Commission, impaneled by and headed by former Representative Barbara Jordan, any type of registry will ultimately require that everyone, citizen and noncitizen alike, would have to present the same information for it to be valid and useful.

In other words, you can't ask just certain people for identification, others not, because we do have laws which respect equal protection of the law. So you cannot ask one person who may look foreign-born for identification, but not ask another person. The other question becomes: How do you deal with the whole issue of self-attestation?

In other words, when you come before an employer, prospective employer, and say to that employer that you are here seeking work, the employer now has to decide if you are eligible to seek the work. Perhaps you may not be a lawful resident alien. And it's up to the employer somehow to determine if that person is going to present authentic identification.

So the question becomes: Do you rely on that prospective employee's word that the person on that ID card is the person before you? The whole issue of self-attestation becomes a very grave issue.

There are some other issues, more in terms of just the whole use of computers and this technology that we have before us and what the implications are. In 1990, the GAO issued a report called "Computers and Privacy: How the Government Obtains, Verifies, Uses, and Protects Personal Data." That report found that of the 910 largest computerized systems containing personal information, 292 were in noncompliance with the Privacy Act.

The report further found that 56 percent of the 910 largest systems in Federal agencies can be accessed by private organizations, such as health care providers, et cetera. The GAO report shows that we don't yet have the type of security that we need in our data bases.

Let me turn now, finally, to the issue of the cost of a verification system or an ID card. I know that we have individuals here, the Commissioner from the Social Security Administration, who can clearly testify, eloquently testify about these issues. But my understanding is that just to reissue our current Social Security cards that we have out there for the Americans, the 260 million—or perhaps a few less—260 million Americans would cost somewhere between $3 billion to $6 billion.

Obviously, if you wish to put a magnetic strip, some form of photo, or fingerprints on this type of card, that would drive up the cost considerably. In fact, apparently we are told that to switch from a paper card to a polyester or plastic card would probably increase the cost tenfold.

So you have a situation where even if you do go to a plastic card that is more secure, with some type of identifier like fingerprints, you're going to have enormous costs, and on top of that you're going to have to constantly change over that card. If someone happens to change a name because of marriage, for example, you now have to reissue that card again.

So on top of all those different concerns, I think that we have to make sure that what we are doing is trying to understand and answer some of the baseline questions that arise whenever we talk about going toward some system where everyone is obligated to provide identification or some group is obligated to provide identification.

Two final points, if I may, Mr. Chairman: Let's keep in mind that right now we have about 44 different valid versions of the Social Security card. We also have a system in this Nation where each State authorizes birth certificates, which may differ from any other State. And we have about 7,000 vital statistics offices which issue these types of birth certificates.

It's important that we understand that whether we go to a system where we're talking about just a registry that may not affect everyone immediately, what we will ultimately end up with is a system where everyone will have to uniformly be checked, so we don't violate privacy, we don't violate equal protection laws, and what we do have is a system where the information is accurate.

So, Mr. Chairman, I just pose those questions. Hopefully, some of the witnesses after me will have a chance to address some of those concerns that I've raised, and I hope that this committee is able to glean additional information that will be helpful in understanding the issue better.

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

PREPARED STATEMENT OF HON. XAVIER BECERRA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Grateful for the opportunity to address the Subcommittee on the very important subject of the integrity of documents issued by the government for the purpose of providing services or work-authorization.

As we consider proposals to produce tamper-resistant documents or a national registry, we must consider whether the policy which we adopt poses risks to our privacy, whether the system we implement is based on clean and accurate data and whether the cost is prohibitive.

ACCURACY OF DATA

Some of the witnesses which you will hear today may argue that a national registry or national ID card will be as convenient and accurate as an ATM machine and PIN code, or a credit card.

> However, Shirley Chater the SSA Commissioner who will be testifying today stated on March 3, at an Immigrations subcommittee hearing "It is not feasible to use the current Social Security card for the purpose of establishing that the person in possession of the card is the person to whom it was issued.

A 1991 Hearing before the Subcommittee on Social Security, of Ways and Means, revealed that data matches by Citicorp and TRW resulted in error rates of 46 percent and 28 percent respectively, due to incorrect data.

> Furthermore, according to a recent New York Times series, the INS runs more than a half-dozen "outdated computer systems which cannot communicate with each other."
>
> According to a recent New York Times series "files get lost . . . and cases get improperly entered at the INS."

A Banking Committee subcommittee hearing in October of 1993 revealed that one million consumers use credit correction or credit restoration services. The American Council on Credit Reporting Accuracy stated:

> The vast proliferation of credit correction and restoration services is a reflection of the poor performance of the credit bureaus that continuously report erroneous and misleading information.

ACCESS AND PRIVACY IMPLICATIONS OF A NATIONAL REGISTRY

A national registry or a national identification card would have to comply with current law, such as the Privacy Act of 1974, and the Computer Security Act of 1987, designed to ensure against unauthorized use and misuse of information.

However, reports and audits by the GAO and the Department of Justice have established that there are serious problems with the quality and availability of data.

According to the Jordan Commission EVERYONE, citizen and non-citizen, would have to "present the same information to be validated."

During testimony offered at a March 3rd hearing of the Judiciary Committee's Subcommittee on Immigration and Claims, Robert Rasor, of the Secret Service, who will be testifying today expressed his skepticism about the need to use a central database.

In 1990 the GAO issues a report *Computers and Privacy—How the Government Obtains, Verifies, Uses, and Protects Personal Data.*

> The report found that of the 910 largest computerized systems containing personal information, 292 were in non-compliance with the Privacy Act.

The report found that 56 percent of the 910 largest systems in federal agencies can be accessed by private organizations such as health care providers, marketing companies, and insurance companies.

In 1990 the GAO issued a report Computer Security—Governmentwide Planning Process Had Limited Impact.

The report found that the plans which were designed by federal agencies to improve security and restrict access had limited impact on "agency computer security programs."

At the time of the GAO report only 38 percent of the 145 plans had been implemented.

The GAO concluded that the government "faces new levels of risk in information security . . ."

In March of 1993 the Department of Justice issued an audit on database access problems at the INS. The databases at the INS contain information necessary to detect, apprehend, and deport criminal aliens, as well as administer employer sanctions provisions.

The audit found that additional access controls were needed, without which the INS' data was vulnerable to "accidental or intentional destruction, modification, disclosure and unauthorized use."

The audit reported on the case of an INS employee who created and altered nearly 2,000 files in exchange for payments as high as $40,000.

The DOJ audit found that INS was vulnerable to "computer fraud", and the possibility that it might be unable to "recover critical data . . ."

In September of 1993 the Department of Justice issued an audit of the INS computer risk analyses and contingency planning. Risk analyses are necessary in order to ensure the security, integrity and confidentiality of data.

The audit found that the INS had still not performed risk analyses of its 24 application systems.

Although the INS had adopted a contingency plan, at the time of the audit, DOJ found that INS' contingency plan had still not been tested at the time of the audit, or approved.

Motor Vehicle Departments routinely sell the information contained in their databases.

THE COSTS OF A NATIONAL VERIFICATION SYSTEM OR NATIONAL ID CARD

Several of today's witnesses may propose that a national registry or national ID card based on the Social Security database is the best way to verify a worker's eligibility.

Such a system would inevitably mean that the SSA data would have to be updated and corrected, and that everyone, citizen and non-citizen alike would have to be interviewed.

According to the Social Security Administration everyone would have to be interviewed in order to reissue 270 million cards, at a cost of $3–$6 billion.

The addition of magnetic stripes, photos or fingerprints would drive up the costs considerably.

Issuing cards to only a portion of the population would save money, but would inevitably leave a significant number of forged cards in circulation.

If more sophisticated cards are produced, for example cards which include holograms, biometric identifiers, or magnetic strips, a system will have to be accessible to employers to verify the information contained in the card.

Who will pay for the equipment which employers will have to utilize?

Polyester or plastic cards, according to the GAO are ten times more expensive to produce than paper cards, and must be replaced every few years due to wear and tear.

OTHER CONCERNS AND QUESTIONS

Proliferation of Cards, Numbers and Identifiers

29 different documents can be used to verify someone's work eligibility and identification.

44 valid versions of social security number cards.

Each State has its own birth certificates, issued from 7,000 vital statistics offices around the country.

In the words of Robert Rasor, there are "thousands of different identifications in use today and personnel reviewing identification need to be able to recognize fraudulent documents. The variety of identification documents makes this impossible."

The Commission on Immigration Reform, the SSA and the INS must first address the proliferation of documents, as well as the extensive forgery of documents before basing a national registry or card on such a system.

Telephone Verification System (TVS)

Some of this afternoon's witnesses may advocate the use of an expanded Telephone Verification System (TVS). The Jordan Commission, in its October report, promoted the TVS, but only as an interim measure.

The commission reasoned that the essential problem with the TVS was that it relied on the prospective employee self-identifying.

Furthermore, representatives of DOJ with whom my office met, conceded that TVS still has substantial "data flow problems" and "data interface problems."

Mr. HORN. Well, that's an excellent overview statement. I think you've stated a series of problems very well. Obviously, the various congressional committees in both the Senate and the House will need to grapple with those.

Representative Maloney.

Mrs. MALONEY. I likewise would like to congratulate you on your statement and thank you for testifying. And I'd like 'o request from the chairman if he would insert in the record a letter to President Clinton, dated September 28, 1994, from Members of the Congressional Hispanic Caucus, opposing a national registry system.

Mr. HORN. Without objection, so ordered.

[The letter referred to follows:]

CONGRESSIONAL HISPANIC CAUCUS,
103rd CONGRESS,
September 28, 1994.

The Honorable Bill Clinton,
President of the United States,
The White House,
Washington, DC 20500

DEAR MR. PRESIDENT: We are writing to express our steadfast opposition to the implementation of a national registry system. As you know, according to testimony before the Senate Subcommittee on Immigration and Refugee Affairs, the U.S. Commission on Immigration Reform is planning to recommend that the Administration immediately initiate a "pilot" worker verification database program in five of the highest immigration-impacted states. We oppose the Commission's proposal because we believe that such a verification system will set us irrevocably on the path to a national ID system.

First, to characterize the Commission's proposal as a test or pilot program is disingenuous and inaccurate. The "test" would cover the five highest immigration impacted states, which are also the five most heavily populated, containing almost 80% of the nation's immigrants, or over 92 million people. In effect, this "test" would require the creation of a national system. The Commission suggests implementing the registry system in some states or for some workers without regard for the high error rate that will result and the devastating consequences that such errors will have for individual workers. A true "test" would analyze the proposals, conduct simulated verification checks on a large, diverse and statistically significant number of mock applicants, evaluate the results, check the error rate, test the privacy safeguards, determine the cost and feasibility of needed modifications and report on these findings. Instead, the Commission appears to be proposing that the residents of some of our largest states be the human "guinea pigs" by which the proposal will be evaluated. That constitutes implementation, not evaluation.

Second, any new system is only as reliable as the information on which it will be based. There are serious problems with the accuracy of the Social Security database, which is the basis for the proposed verification system. According to a 1992 report by the Senate Subcommittee on Immigration and Refugee Affairs, over 60% of social security cards were issued without proof of the individual's identity or citizenship. Even if the security of the card and the database are improved, the documents used to obtain such a card—birth and baptismal certificates, drivers licenses, and school and medical records—can be forged. While call-in systems are regularly used to make credit card purchases, matching projects by Citicorp and

TRW resulted in error rates due to incorrect or unverified Social Security numbers of 46% and 28% respectively.

The Immigration and Naturalization Service (INS) database is equally, if not more, flawed. Recent evidence demonstrates that the INS routinely fails to enter records of work-eligible individuals into its computers, that the data in the computers are incomplete, and that the agency fails to update its records with critical relevant information. In fact, a March 1993 Department of Justice audit of access to the INS database found that without "additional controls, INS' data is vulnerable to either accidental or intentional destruction, modification, disclosure and unauthorized use." The American Civil Liberties Union (ACLU) is litigating a case in Los Angeles where INS authorities have admitted to losing the files of 60,000 people, which may have resulted in routine, justified denial of work authorization. In our view, it is irresponsible to recommend implementing a system based on such manifestly deficient data.

Third, such a verification system will not only be unreliable, but it is nearly impossible to implement effectively without requiring a unique individual identifier. How else will individual workers prove that the social security numbers they present belong to them? Numbers are easily forged or stolen, as occurs with other documents currently in use. Attorney General Janet Reno recently expressed concern over the Commission's expected recommendation since widespread counterfeiting could cause such a plan to "backfire." Therefore, the system would be ineffective unless it relies on an identifier to tie the worker to the number. Options include a "Counterfeit resistant" identification card based on a drivers license or social security card, or the issuance of a PIN number to every worker. Thus, despite claims to the contrary, a worker verification system must necessarily include the creation of a national ID card. And all of these options would still be subject to fraud.

Fourth, a verification system will also have negative consequences on individual privacy and civil rights. Privacy is threatened since the Social Security number is already widely used. A national verification or ID system would have to contain substantial private identifying information. Furthermore, it would be impossible to control who has access once the system is in place. The Heritage Foundation states that we are already on a collision course towards Big Brother "by requiring that every American have a national identification card—or work permit—issued by a federal bureaucracy."

Further, such a system would cause widespread discrimination against those who look and sound foreign. A 1990 report by the U.S. General Accounting Office indicated that nearly 20% of employers nationwide have adopted discriminatory behaviors resulting from employer sanctions. Implementation of a national identification card will only widen that great potential for continual status checks by employers, police, banks, landlords, and merchants against foreign-looking and -sounding, persons. The victims would be citizens and legal immigrants who work hard, pay taxes, and play by the rules.

Last, in addition to its highly discriminatory effects and limitation on personal freedom, a national verification system would be extremely costly. According to the Social Security Administration, the creation of a universal "employment card" would cost nearly $2.5 billion. This does not include the technological costs involved in computerizing a verification system, cleaning up the database, and the costs of issuing cards to every applicant and replacing lost cards.

It is important to enforce our nation's immigration laws and protect our borders. However, a national identification system's effectiveness in deterring unauthorized employment or reducing the flow of undocumented immigration is highly doubtful. Employer sanctions have failed to control undocumented immigration partly because the labor market for undocumented immigrants has not changed. Employers who "benefit" from the hiring of unauthorized workers do so by intentionally violating the employer sanctions law in order to exploit employees in violation of minimum wage and hour laws. That problem will not be remedied by a national registry or identity card system. Employers intent on violating the sanctions law will continue to do so.

For these reasons, we strenuously oppose implementation of a worker verification system.

Sincerely,

LUCILLE ROYBAL-ALLARD,
ED PASTOR,
RON DE LUGO,
FRANK TEJEDA,
NYDIA VELÁZQUEZ.

Mr. BECERRA. Thank you, Mr. Chairman.

Mr. HORN. Thank you for coming.

In deference to Representative Becerra's schedule, I did not have either Representative Maloney or myself make an opening statement, which we will do now. I have a brief one.

The subcommittee is meeting today to solicit from interested parties suggestions for improving the integrity of documents that entitle people to gain public benefits or to be hired for work. A Commission on Immigration Reform, headed by former U.S. Representative Barbara Jordan, made several recommendations last fall for restoring credibility to the Nation's immigration policy.

The commission cited widespread counterfeiting of documents acceptable for verification of identity and employment authorization as a factor undermining the current process. It recommended development of a "simpler, more fraud-resistant system for verifying work authorization."

In the President's 1996 budget, the administration proposes to reform the nation's immigration process, in part through development of a nationally available employment verification system. Such a system very likely will depend heavily on the accuracy of a supporting data base, and will rely even more critically on the integrity of documents used to inquire against it.

Today, we will hear from several qualified witnesses with varied experiences in matters that relate to document and data base integrity. I look forward to everyone's testimony and to working with all of you on how best to fix what is wrong with our system for verifying benefit entitlements and work authorization.

May I say that I have had a longstanding interest in this, and I will insert this as part of my statement: a dissent and additional statement I filed in 1980, as vice chairman of the U.S. Commission on Civil Rights. I noted that, on August 4, 1977, the Carter administration proposed a package of legislative proposals to reform our immigration laws. One of the key recommendations was the call for employer sanctions to make illegal the hiring of so-called "undocumented workers."

Various ethnic communities quite properly expressed concern that employers might be reluctant to hire those with a shade of skin other than white for fear that they were undocumented workers and illegal aliens. In brief, the administration left out the essential element which is key to a fair employer sanctions policy, and that is what some have described as a "secure" or "counterfeit-proof" Social Security card.

I agree with that criticism. If we are to deal with reality and not find ourselves still discussing this matter a decade from now, while millions of American citizens continue to be denied job opportunities, then the establishment of such a secure and counterfeit-proof Social Security card for any who wish to be employed must be a first order of business on the national legislative agenda. That was 1980. It is now 1995. I was wrong about the decade discussion; it's a decade and a half discussion.

So here we are, and without objection the full statement will be added to my opening statement.

[The prepared statement of Hon. Stephen Horn follows:]

PREPARED STATEMENT OF HON. STEPHEN HORN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

The Subcommittee on Government Management, Information and Technology will come to order.

The Subcommittee is meeting today to solicit from interested parties suggestions for improving the integrity of documents that entitle people to gain public benefits or to be hired for work.

A commission on immigration reform headed by former U. S. Representative Barbara Jordan made several recommendations last fall for restoring credibility to the nation's immigration policy. The commission cited widespread counterfeiting of the documents acceptable for verification of identity and employment authorization as a factor undermining the current process. It recommended development of a "simpler, more fraud-resistant system for verifying work authorization."

In the President's 1996 Budget the Administration proposes to reform the nation's immigration process, in part through development of a nationally available employment verification system. Such a system very likely will depend heavily on the accuracy of a supporting database and will rely even more critically on the integrity of documents used to inquire against it.

Today we will hear from several qualified witnesses with varied experiences in matters that relate to document and database integrity. I look forward to everyone's testimony and to working with all of you on how best to fix what is wrong with our system for verifying benefit entitlements and work authorization.

ADDITIONAL PREPARED STATEMENT OF HON. STEPHEN HORN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

"THE TARNISHED GOLDEN DOOR" CIVIL RIGHTS ISSUES IN IMMIGRATION—A REPORT OF THE UNITED STATES COMMISSION ON CIVIL RIGHTS, SEPTEMBER 1980

Civil Rights in Immigration

Nothing is more pitiful than a nation which stands helpless and immobilized when it should meet the needs of its own citizens and lawful residents. Yet that is exactly what is happening with respect to the lack of an effective national policy concerning the illegal aliens who are coming to this country to seek employment and a better life for themselves. Calling them by the euphemistic phrase "undocumented workers" does not make their entry any less illegal nor reduce their impact on employment opportunities for our own citizens. As Secretary of Labor Tay Marshall noted on December 2, 1979:

> If only half, or 2 million of them are in jobs that would otherwise be held by U.S workers, eliminating this displacement would bring unemployment down to 3.7%, which is below the 4% full-employment target set by the Humphrey-Hawkins Act.[1]

It should be clear that the illegal alien problem is not simply an Hispanic problem and is not limited to the five Southwest States; it is a national problem.[2] If one examines the employment situation in the North-Central States, in New England, and along the eastern seaboard, one can readily find thousands of non-Hispanic illegal aliens widely employed in both the large industries and the small businesses of those areas. As the Vice President's Task Force on Youth Employment concluded:

[1] Harry Bernstein, "Illegal Aliens Cost U.S. Jobs—Marshall," an interview with Secretary of Labor F. Ray Marshall, Los Angeles Times, Dec. 2, 1979, p.I–1.

[2] Very simply, the estimate of illegal aliens is uncertain except that it is at least several million. Lawrence Fuchs, Director of the Select Commission on Immigration and Refugee Policy, has claimed that there are no more than 6 million undocumented workers and that no more than 50 percent of them are Mexican. Prof. Vernon M. Briggs, Jr., of Cornell, has also estimated that "it is unlikely that Mexicans account for no more than half of the annual flow of illegal aliens into this country." Vernon M. Briggs, Jr., "The Impact of the Undocumented Worker on the Labor Market," in The Problem of the Undocumented Worker (Albuquerque, N. Mex.: Latin American Institute of the University of New Mexico, n.d.), pp. 31–38, p. 33. In August 1978, the Denver Post reported a belief of the Mexican Ambassador to the United States, Hugo D. Margain, that without guest worker programs such as the so-called bracero program that there could be as many as 10 million illegal aliens in this country. ("Our Undocumented Aiens—Part Four, A National Debate What To Do?" in Empire Magazine, the Sunday magazine of the Denver Post, Aug. 6, 1978.) Estimates of illegal aliens in the United States have ranged from 3 to 12 million. For 1985 Lesko Associates estimated 8.2 million illegal aliens, of whom 5.7 million were estimated to be Mexican. The U.S. National Commission for Manpower Policy concluded that the average illegal alien population in 1977 was probably within the range of 3 to 6 million persons.

"Estimates on the percentage of undocumented workers in the U.S. labor force range from 2 percent to as high as 10 percent."[3]

There is no doubt that the illegal aliens who are employed in the garment firms of Los Angeles, in the restaurants of the District of Columbia, or in the automobile factories of Detroit are hard working. Often they seek not only a better life for themselves, but also for those they have left behind in their native lands—families and relatives to whom they frequently send funds.[4] But as a matter of American national policy, citizens and lawful residents should not be left unemployed because the governments from which these illegal aliens flee are not meeting the economic needs or facing the population problems of their own people.

This Nation should be particularly concerned with the distressing working conditions in the low-skill, low-wage industries in which illegal aliens are employed and with the resultant denial of job experiences for our own citizens. It is a serious problem when entry level job experiences are denied to inner-city youth because these jobs are increasingly occupied by illegal aliens subject to the exploitation and fear created by unscrupulous employers and sometimes connived in by labor unions. Some have argued that Americans will not fill low-status, low-wage jobs and therefore illegal aliens are necessary if the work is to be done.[5] This is simply untrue. Such "we need them and they are happy here" arguments were last heard to justify plantation slavery before the Civil War.[6] The fact is that in each occupational category a majority of the positions are filled by American citizens. If workers are truly needed to perform specific seasonal tasks, then guest worker programs such as those utilized in various European countries might be instituted. Under such programs there could at least be a regularized procedure to assure the entry of needed workers to perform specific types of jobs (but not limited to a specific employer). Such a procedure would also ensure full payments and fringes, health clearance, and other accepted American practices too often neglected as some employers victimize the illegal alien as well as the broader public interest. It is clear that the problem of illegal immigration is a political as well as a human and a legal issue. That neither the Congress nor the President has faced these issues is tragic.

The Border Patrol has a difficult and dangerous task. It is understaffed and its members are underpaid. As one careful student of the subject has observed ". . . the legal immigration system of the United States has been rendered a mockery . . . ."[7]

There is big money and individual misery in the smuggling of illegal aliens across the American borders. Because our borders are largely unpatrolled and most illegal entrants can melt into our society, we are an attractive target, especially for those who come from Mexico where the government has failed to address the needs of its own people through either a sound economic or population policy. It is hoped that some of the billions of dollars now available within Mexico as a result of the development of its petroleum resources will go toward the development of labor-intensive food processing and textile industries in the northern states of that nation. Certainly the American Government has a stake in also providing appropriate assistance to encourage such a development. Increasingly unemployed American workers should not be the only form of foreign aid available to Mexico.

For those who seek to count illegal aliens to increase their political power, perhaps it would be wise to recall *Mathews* v. *Diaz,* 426 U.S. at 82, in which the Court

[3] The White House, A Summary Report of The Vice President's Task Force on Youth Employment (1980), p. 19.

[4] In the case of Mexico, it is estimated that the return of American dollars by illegal aliens in the United States is the largest dollar earner for Mexico—ahead of the dollars gained from American tourism. Wayne A. Cornelius, "Illegal Mexican immigration to the United States: a Summary of Recent Research Findings and Policy Implications," p. 14.

[5] The findings of the 1979 National Longitudinal Survey (NLS) of Youth Labor Market Experience refute this myth: "Substantial numbers of youth are willing to work at less than the minimum wage. This extensive longitudinal study found that the youth unemployment rate (38.8% for black youth and 16.6% for white youth) was 37% higher than had been shown by the Current Population Survey monthly sample." The New York Times, Feb. 29, 1980, pp. A1 and A14.

[6] Professor Briggs has commented that, "No U.S. worker can compete with an illegal alien when the competion depends upon who will work for the lowest pay and longest hours and accept the most arbitrary working conditions. It is self-serving for employers to hire illegal aliens and claim simultaneously that no citizen workers can be found to do the same work. In the local labor markets where illegal aliens are resent, *all* low-income workers are hurt. Anyone seriously concerned with the working poor of the nation must include an end to illegal immigration as part of any national program of improved economic opportunities." (emphasis supplied) Vernon M. Briggs, Jr., "The Impact of the Undocumented Worker on the Labor Market," in The Problem of the Undocumented Worker, p. 34.

[7] Ibid., p. 32.

noted that "Congress has no constitutional duty to provide all aliens with the welfare benefits provided to citizens. . . ."

Residents from my own State of California certainly stand to profit from counting illegal aliens and thus gaining a few more seats in the House of Representatives. But should foreign citizens—many of whom are transient and subject to deportation—be the basis of our representation process? Is it fair to the legitimate political interests of citizens in the North and the East (where there are probably proportionally less illegal aliens than in the Southwest) not to have their votes counted effectively in the formulation of national policy through that representative process simply because some States happened to have an enhanced apportionment as a result of the substantial presence of illegal aliens?

On August 4, 1977, the Carter administration proposed a package of legislative proposals to reform our immigration laws. One of the key recommendations was the call for employer sanctions to make illegal the hiring of so-called undocumented workers. Various ethnic communities quite properly expressed concern that employers might be reluctant to hire those with a shade of skin other than white for fear that they were undocumented workers and illegal aliens. In brief, the administration left out the essential element which is a key to a fair employer sanctions policy and that is what some have described as a "secure" or "counterfeit-proof" social security card.[8] I agree with that criticism. If we are to deal with reality, and not find ourselves still discussing this matter a decade from now while millions of American citizens continue to be denied job opportunities, then the establishment of such a secure and counterfeit-proof social security card for any who wish to be employed must be a first order of business on the national legislative agenda.

With this exception, I have supported the recommendations for due process which we have made in the attached report—although at times I have felt that some of our proposals, if enacted, should be best described as "the Immigration Attorneys Relief Act of 1980."

STEPHEN HORN.

Mr. HORN. Representative Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman, and thank you for calling this hearing on the integrity of Government documents.

This hearing potentially has a very broad scope, which includes the impact of advancing technology on the availability of information to both the Federal Government and the private sector, the prospects for developing some form of a national identification card, controls on illegal immigration, and the general prevention of fraud.

[8] Gerda Bikales, program associate for Population/Immigration, National Parks & Conservation Association, has made an effective case for such a card in "The Case for a Secure Social Security Card" (September 1978). 18 pp., available from National Parks & Conservation Association, 1701 13th Street, N.W., Washington, D.C. 20009. She notes that, "The Social Security card and the driver's license enjoy primary credibility as general purpose identification. . . ." (p. 9) "Forty-four States now affix a photograph of the driver on the license adding to the security of the document. . . ." (p. 10) Observing that 41 State jurisdictions now issue "impressive and offical looking identification cards to non-drivers." Bikales adds that, "The dreaded I.D. has been brought in through the back door, by popular request!" (p. 11) She observes that "it is almost inconceivable how anyone could be damaged by revealing [bona fide legal residency in the United States]; on the contrary, it is universally acknowledged to be a highly advantageous quality, one that many millions all over the world are desperately trying to take on as their own." (p. 14) She favors "an upgraded Social Security card" as "the least drastic alternative" (p. 14) and recalls that in July 1973, the Report [Records, Computers and the Rights of Citizens] of the [HEW] Secretary's Advisory Committee on Automatic Personal Data Systems "provide further assurance that Social Security numbers were legislatively intended by the Congress 'to be available for use in preventing aliens from working illegally and public assistance beneficiaries from receiving duplicate or excessive payments.' " Ibid., p. 121.

Another strong advocate "an identification system which would apply to all workers" is Secretary of Labor Ray Marshall. He believes that "a noncounterfeitable Social Security card could be issued to all workers changing jobs and to all newly hired persons, and that could be done for under $200 million. . . ." Harry Bernstein, "Illegal Aliens Cost U.S. Jobs—Marshall," an interview with Secretary of Labor F. Ray Marshall, Los Angeles Times, Dec. 2, 1978, p. I–1. Considering that The United States Budget in Brief—Final Year 1981 indicates (p. 52) that "unemployment recipients are estimated to average 2.9 million per week in 1980 and 3.4 million per week in 1981" with outlays for unemployment compensation estimated to increase $3.2 billion "from $15.6 billion in 1980 to $18.8 billion in 1981," a $200 million investment to open up perhaps millions of jobs for citizens and permanent residents is a very cheap investment indeed.

We need to keep our focus on this question: How can information best be used to meet society's needs, while protecting individual freedom and privacy?

We can all agree that one of the proper roles for Government is to use information about individuals to ensure that the laws are obeyed, and to prevent fraud and abuse. We will hear from the Social Security Administration and from the Immigration and Naturalization Service about how they can use information to achieve these goals and the problems they encounter while doing so.

Members of Congress want to ensure the ability of government to carry out its responsibilities under the law; we do not want the government to go too far in employing new technology. The American people's right to privacy must be maintained.

During this hearing, we will hear about advances in technology which might soon make it possible to encode a vast amount of information on a small plastic card, including such data as a Social Security number, fingerprints, and medical background. Many Americans are concerned about the creation of a national identity card which could track them from cradle to grave. Others welcome it as a convenience and for simplicity.

We must all take steps to ensure the reliability of the data bases which might be used to create some form of national identifier. Questions have been raised about the dependability of the files of the Social Security Administration, the Internal Revenue Service, and other Federal agencies. We already know that the current Social Security number, which has become a sort of de facto national identifier, may not really be suited to that purpose.

Some have advocated the use of biometrics, such as fingerprints, photographs, or DNA, to provide a unique identifier for every person, while at the same time protecting personal privacy. It will be interesting to see whether these potentially conflicting goals can be achieved and at what cost.

Mr. Chairman, I hope we can have a broad-ranging discussion today. It is tempting to focus on the technology and mechanics of how a national identification system might work, and those issues should be carefully explored, but we must also ask ourselves how far we really need to go in this area and be wary of the consequences of going too far.

Mr. Chairman, I request that you insert in the record a letter, dated March 1, 1995, which I received from Frances C. Berger, chair of the Committee on Immigration and Nationality Law of the Association of the Bar of the city of New York. The letter expresses reservations about the proposal by the U.S. Commission on Immigration Reform for the creation of a computerized national registry to verify the employment authorization of all workers. I request that it be part of the record.

Mr. HORN. Without objection, it will be part of the record.

Mrs. MALONEY. Thank you.

[The letter referred to follows:]

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK,
NEW YORK, NY
March 1, 1995

The Honorable Carolyn B. Maloney
United States House of Representatives
1504 Longworth Office Building
Washington, D.C. 20515

Re: National Computerized Employment Registry

DEAR CONGRESSWOMAN MALONEY: On behalf of the Committee on Immigration and Nationality Law of the Association of the Bar of the City of New York, we write to express our grave concerns with respect to the U.S. Commission on Immigration Reform's recent proposal for the creation of a computerized national registry to verify the employment authorization of all workers. In this Committee's opinion, the proposal should be rejected for the following reasons: absent an expensive and lengthy effort to improve the registry's database, it would be too inaccurate to be trustworthy; it would increase the occurrence of discrimination against foreign-appearing U.S. citizens and lawful permanent residents; and it would unreasonably intrude upon the privacy of all Americans.

The Commission's proposal calls for a verification system based upon Social Security Administration ("SSA") and Immigration and Naturalization Service ("INS") information, yet both agencies have publicly admitted that their databases are incomplete, inaccurate and unreliable. The Commission has already received extensive evidence of the tragic recordkeeping deficiencies of both agencies. Nevertheless, even though the Commission's report recognizes this is a major problem, it has not provided a sufficient explanation as to how this deficiency may be overcome. At a minimum, we believe the Commission should recommend extensive simulation-testing of computer registry prior to the implementation of any "pilot projects". We cannot condone the immediate implementation, even on a limited basis, of an inherently unreliable system at the expense of individuals who would suffer great personal hardship while flaws in the system are worked out. In our opinion, the goal of reducing illegal immigration to this country will not be furthered by hastily implementing an ill-conceived system in which U.S. citizens will inevitably be denied work authorization due to a computer "glitch". Without a highly accurate database, the concept of a computerized employment registry is fatally flawed and, ultimately, doomed to failure.

Moreover, this Committee is deeply skeptical of any estimates which would imply that those pervasive database problems may be corrected by spending a relatively modest amount. For the computer registry to be reliable, both the INS and SSA databases must be thoroughly cleansed of inaccuracies and steps must be taken to reduce access to fraudulent "breeder documents" (i.e. documents, such as birth certificates, which are used to obtain access to INS and SSA benefits). The Social Security Administration indicates a requirement of $300 million over five years to create the requisite database. Even if we assume that this estimate is accurate, it does not include the amount necessary for INS to create a sufficiently reliable database nor does it include the cost of making "breeder documents" more counterfeit-resistant. Additionally, if a counterfeit-resistant identity card, possibly a new social security card, is issued as a primary method of verifying identity in the proposed system, it has been estimated that the total cost of the registry would increase by approximately $2.5 billion. It is this Committee's position that the creation of a multi-billion dollar registry program to target approximately 1.5% of the U.S. population is an extremely costly alternative which is unlikely ever to achieve its primary objective.

In addition, we are concerned that the computerized national employment registry will directly cause increased discrimination against U.S. citizens, lawful permanent residents and other lawful U.S. workers. If the registry requires an application or re-registration process, foreign-appearing persons applying for inclusion into the registry are likely to undergo greater scrutiny and face wide-scale discrimination from skeptical administrators in charge of the application process. Many legal immigrants and foreign-appearing citizens may be denied or delayed entry into the registry solely because of their appearance and ethnicity. Additionally, if a counterfeit-resistant identity card is created, it is likely that it will be abused in a myriad of situations outside the employment context. Given the current anti-immigrant sentiment in this country, it is reasonable to anticipate that foreign-appearing persons will be routinely asked to present this identity document by police officers, landlords, bank officials, state/local government employees, etc. regardless of any restrictions on its use imposed by Congress. The ability to provide such an identity document when reguested does not lessen the stigma and discrimination that will be suffered by these individuals.

Moreover, this Committee is troubled by the likelihood that the proposed computer registry will cause further intrusions into individual privacy. A national registry would pose a substantial threat to the individual privacy of all U.S. residents in that it would be widely accessible to private entities, thus substantially increasing the risk of unauthorized disclosure of personal information. In the likely event that a counterfeit-resistent identity card is created, it could quickly take on the attributes of a national ID card, which could easily become the country's sole identifier for a broad range of purposes. A requirement that every American possess a single type of identification document, issued by a federal bureaucracy, brings this country ever closer to the "Big Brother" society that has always been antithetical to the traditions upon which this nation was founded.

We also question the fundamental proposition that the computerized registry will reduce the "employment magnet" and thus reduce illegal immigration. We concur with those groups, including the Congressional Hispanic Caucus, who doubt that a computerized registry system will have a significant impact upon unauthorized employment or illegal immigration. Employers who have ignored the employer sanctions provisions of the law will ignore the registry and will continue to employ, at substandard wages and working conditions, undocumented workers seeking a better life for themselves and their families in the United States. Rather than creating a computerized registry, this Committee believes that resources and attention should be focused on the enforcement of existing labor laws and the creation of international economic initiatives through a foreign policy that will reduce the underlying causes of unauthorized migration to the United States.

We commend the Commission for inclusion of both recommendations in its report to Congress and look forward to greater emphasis on these areas as the debate on immigration policy moves forward.

This Committee expressed its concerns regarding a national identifier in the form of an identity card, social security card or computer registry, in 1989 when it examined findings of discrimination resulting from the employer sanctions provisions of the Immigration Reform and Control Act of 1986. We reaffirm our earlier conclusion that a national identifier is an ill-advised response to the issue of unauthorized immigration.

Should you require additional information with respect to our position on this proposal, we would be pleased to meet with you to discuss this matter further at your convenience.

Thank you for your attention.

Very truly yours,

FRANCES C. BERGER,
Chair.

Mr. HORN. Thank you.

Let me just state the ground rules before the first panel comes forward.

When the witnesses come forward, we will automatically enter your full statement in the record, and we would very much appreciate it, if you would summarize your statement in 5 minutes. You will see a green light for 4 minutes. It will go to yellow from 4 to 5. We would appreciate your stopping at the end of that, and then we can pick up in questions the parts you might not have had a chance to mention. We are fairly liberal, between the two of us, on making sure we get out of each witness all that you have to tell us.

The other practice of the Committee on Government Reform and Oversight is to swear in witnesses. So if the first panel will come forward, we will swear you in and begin the testimony. We will take a break after the first 5-minute testimony is over, so we can get over to vote and then come back. We apologize. We think there are only two more votes today.

We have Mr. Hill, Ms. Martin, Mr. Puleo, Mr. Nahan, Mr. Epstein, Commissioner Chater, and Mr. Velde. There is a sign there for each of you.

[Witnesses sworn.]

Mr. HORN. All witnesses affirmed.

Very well, I'd like to start with Mr. Hill, who is a member of the U.S. Commission on Immigration Reform; and Susan Martin accompanies him, who is the Executive Director of the U.S. Commission on Immigration Reform.

Mr. Hill.

STATEMENT OF ROBERT CHARLES HILL, MEMBER, U.S. COMMISSION ON IMMIGRATION REFORM, AND SUSAN MARTIN, EXECUTIVE DIRECTOR, U.S. COMMISSION ON IMMIGRATION REFORM; JAMES A. PULEO, EXECUTIVE ASSOCIATE COMMISSIONER FOR PROGRAMS, IMMIGRATION AND NATURALIZATION SERVICE, ACCOMPANIED BY JOHN NAHAN, DIRECTOR OF SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS BRANCH, AND GIDEON EPSTEIN, SENIOR FORENSICS ANALYST, FORENSICS DOCUMENTATION LABORATORY

Mr. HILL. Mr. Chairman, Representative Maloney, members of the subcommittee, on behalf of Professor Barbara Jordan, our chair, and my fellow members of the U.S. Commission on Immigration Reform, I want to thank you for this opportunity to testify before you today.

Dr. Susan Martin, Executive Director of the Commission, is here with me to assist in answering any questions you may have.

In our first report to Congress last fall, entitled "U.S. Immigration Policy: Restoring Credibility," we sought to recommend a comprehensive strategy to control illegal immigration. Because I have submitted written testimony for the record, let me just sum up a few points regarding our proposals for development of a more efficient system for verification of employment authorization and the reliability of government documents in this critical area.

First, in order to prevent employment of persons not authorized to work in the United States, while ensuring that Americans and other legitimate workers are not discriminated against, we simply must develop and implement a better system to verify work authorization at the work site.

Let me be very clear. The verification system we now have, the I–9 process, does not do what it was supposed to do. It does not effectively deter the employment of illegal aliens. What it does do, we don't want; namely, is to burden businesses with paperwork while creating abundant opportunities for fraud and forgeries. It may even provide an excuse for, if it does not actually provoke, discrimination against American workers who happen to look or sound foreign.

The Commission staff has provided each member of the subcommittee with a copy of the I–9 form, in case you are not familiar with it. At the root of these problems with the I–9 is the proliferation of counterfeit documents. During our investigations, the Commission learned that illegal aliens can now purchase counterfeit drivers' licenses and Social Security cards for as little as $25.00. A green card is slightly more expensive.

Moreover, we also learned that counterfeits of any document, even the most tamper-resistant, would soon be available on the open market, largely through the innovation of desktop publishing.

These cards could easily pass a visual check, particularly by employers who are not trained to spot counterfeits.

The Commission recommendation is that we develop and implement a better system for work site verification. We recommend immediate testing of the most promising option: a computerized registry based on the Social Security number.

For decades, all workers have been required to provide employers with their Social Security number. Depending on the results of pilot projects that are now being designed, the cumbersome I–9 process, with its dozens of documents and blizzard of paper, could be replaced by a single electronic step to validate information every worker must already provide.

While there are many ways to test that system, the key is that electronic validation does not necessarily depend on documents at all, so it will not be as vulnerable to fraud as the I–9. Because all workers must present the same information to be validated, employers will not be as likely to discriminate, even inadvertently. The only thing to ask a prospective employee would be, "What is your Social Security number?" and everyone already provides that information now. The government already has the data it needs on the Social Security and INS data bases. There needs to be improvement, of course, particularly at the INS, but cleaning up those data bases is something that we should be doing already.

This Commission expects to have meaningful results from the initial phases of pilot testing of the electronic verification system by 1997. We will incorporate these results into our final report to Congress so that we can make an informed recommendation on whether that system should be implemented nationwide, with particular attention to civil liberties and privacy concerns.

While we on the Commission are certainly not computer systems experts and never pretended to be, we do recognize "garbage in, garbage out." Clearly, people who obtain real documents through false pretenses pose a problem. This is true, even though the Social Security Administration does a face-to-face interview and document check on every adult who seeks a Social Security number, since nowadays most children receive numbers shortly after birth.

Accordingly, we made recommendations for reducing fraudulent access to the so-called "breeder documents," particularly birth certificates that can be used to establish an identity in this country.

We recommend certain basic steps: standardized application forms for birth certificates, interstate and intrastate matching of birth and death records, Federal agencies' acceptance of only certified copies of birth certificates issued by States, standard design and paper stock for all certified copies of birth certificates to reduce counterfeiting, and computerization of State birth records depositories.

The Commission also recommends imposition of greater penalties on those producing or selling fraudulent documents. RICO provisions to facilitate racketeering investigations should also cover conspiracy to produce and sell fraudulent documents.

Let me add a tentative note about costs associated with our proposals for a verification system. The Social Security Administration made preliminary estimates for the Commission of its cost of a telephone verification program to validate Social Security numbers: $4 million over the first 2 years for design and development; annual cost of $32 million for maintenance and operation. Resolution of discrepancies referred to the Social Security Administration were estimated to cost $122 million initially and $30 million per year thereafter.

So the total cost of the registry over 5 years, according to the Social Security Administration, would be approximately $300 million. By way of comparison, the Urban Institute estimated that illegal aliens cost seven States alone more than $2.1 billion a year. Other scholars have put the costs associated with illegal immigration much higher. Spending $300 million over 5 years to save $2 billion or more each year is a sound investment.

One final point I would like to make: The key to our work at the Commission on Immigration Reform so far has been that through intense discussions and studies we have managed to arrive at a bipartisan consensus. We hope to continue that record.

I would be glad to answer any questions.

[The prepared statement of Mr. Hill follows:]

Prepared Statement of Robert Charles Hill, Member, U.S. Commission on Immigration Reform

Mr. Chairman and Members of the Subcommittee, on behalf of Professor Barbara Jordan, our Chair, and my fellow members of the U.S. Commission on Immigration Reform, I want to thank you for this opportunity to testify.

In our first report to Congress last fall, entitled U.S. Immigration Policy: Restoring Credibility, we sought to recommend a comprehensive strategy to control illegal immigration. Growing frustration about it undermines our first commitment to legal immigration in the national interest.

We simply must develop a better system for verifying work authorization. Reducing the employment magnet is the linchpin of a comprehensive strategy to reduce illegal immigration. Illegal aliens are here for jobs. That is the attraction. So the only effective way to deter illegal immigration must include the worksite. The reliability of government information is critical to this effort.

The system we have now, the I–9 process, is doubly-flawed. It does not do what it was supposed to do, namely deter the employment of illegal aliens. What it does do, we do not want—namely, burden businesses with paperwork, while creating abundant opportunities for fraud and forgeries. It may even provide an excuse for, if it does not actually provoke, discrimination against workers who happen to look or sound foreign.

At the root of these problems is the proliferation of counterfeit documents. During our investigations, the Commission learned that illegal aliens can now purchase counterfeit drivers licenses and social security cards for $25. A green card is slightly more expensive. Moreover, we also learned that counterfeits of any document—even the most tamper-resistant—would soon be on the black market. These cards could easily pass a visual check, particularly by employers who are not trained to spot counterfeits.

Honest employers are caught between the proverbial rock and a hard place. Because the system is based on documents, employers are placed in a position of making judgments many do not feel qualified to make.

Identifying forgeries is difficult, even for trained professionals. If an employer accepts false documents presented by an unauthorized worker, that employer is vulnerable to employer sanctions for having hired someone under false pretenses, regardless of the fact that they may well have been fooled themselves. Yet if an employer chooses to doubt particular documents, and asks for more from some workers and not from others, that is discrimination.

The Commission believes that the way to develop a better system of worksite verification is to immediately test the most promising option. After examining a wide range of alternatives, the Commission concluded that the most promising option for secure, non-discriminatory verification is a computerized registry based on the Social Security Number.

For decades, all workers have been required to provide employers with their Social Security Number. Depending on the results of pilot projects that are now being designed, the cumbersome I-9 process, with its dozens of documents and blizzard of paper, could be replaced by a single electronic step to validate information every worker must already provide.

The Commission also looked at the feasibility and effectiveness of reducing the number of documents used in verification. Again, we support such efforts as interim measures. But the fatal flaw here is the vulnerability of all documents to counterfeiting. We heard expert testimony that any document, even the most tamper-proof ones, can be forged so well that only experts can identify the fakes. Employers cannot be expected to identify counterfeit documents.

The Commission believes electronic validation of the Social Security Number is the most promising option because it holds great potential for accomplishing the following:

- Reduction in the potential for fraud. Using a computerized registry, rather than relying on documents, guards against counterfeits.
- Reduction in the potential for discrimination. All workers must present the same information to be validated.
- Reduction in the time, resources and paperwork spent by employers in complying with IRCA. INS employees who now chase paper could be redirected to chase down those who knowingly hire illegal workers.

The Commission did not try to micromanage the Executive branch's implementation of this recommendation in advance. We deliberately did not spell out precisely how the software of the registry would be designed, although we did specify that just six pieces of information seem necessary: name, Social Security Number, place and date of birth, mother's maiden name and status code. Nor did we limit the innovation that might be applied in pilot projects to test the registry.

There must be objective, systematic evaluation of the pilot programs. This Commission expects to have meaningful results from the initial phase of pilot testing by 1997. We will incorporate these results in our final report to Congress, so that we can make an informed recommendation on whether that system should be implemented nationwide, with particular attention to civil liberties and privacy concerns. The features of pilot programs should include:

- A means by which employers will access the verification system to validate the accuracy of information given by workers. We received conflicting testimony about the best way to ascertain that a new hire is who he or she claims to be. Some believe that the tamper-resistant driver's licenses now being issued by many states can do the job; others strongly advocate testing a more secure Social Security card.

  But it is also possible that electronic validation through a telephone system would require no document at all. Every ATM system uses a PIN number to protect our money. We should test to see if personal information, such as the mother's maiden name and date of birth, that is already part of the Social Security database, can serve the same function for worksite verification.
- Measures to ensure the accuracy of the necessary data. Improvements must be made in both the INS and Social Security Administration databases to ensure that employers have timely and reliable access to what they need. Frankly, no one can be opposed to improving the reliability of the data in these agencies. There is no protection of liberty in government error.
- Measures to ensure against discrimination. One key to the Commission's recommendation is that employers would no longer have to ascertain whether a worker is a citizen or an alien, native-born or an immigrant. All workers would have to present the same information to be validated.
- Measures to protect civil liberties. Explicit protections should be devised to ensure that the registry is only used for its intended purposes. The Commission believes that electronically validating the Social Security Number could be used to ascertain eligibility for public benefits, without damage to civil liberties, because everyone receiving public assistance must already present a Social Security Number just as they do for work. But the registry is not to be used for routine identification purposes, and there must be penalties for inappropriate use of the verification process. The Commission's unanimous, unequivocal view is that no one should be required to carry a document and produce it on demand to prove their right to be here.
- Measures to protect privacy. Explicit provisions must also be built into the system to safeguard individual privacy. The information contained in the registry will be minimal, given its limited purpose. But the Commission is aware that while access to any one piece of information may not be intrusive, in combination with other information it can lead to privacy violations.
- Estimates of the start-up time and financial and other costs. The Social Security Administration made preliminary estimates for the Commission of its cost for pilot projects: $4 million over the first two years for design and development; and annual costs of maintenance and operation of $32 million. Discrepancies referred to

the Social Security Administration were estimated to cost $122 million initially, and $30 million per year thereafter. So the total cost of the registry over five years, according to the Social Security Administration, would be approximately $300 million.

By way of comparison, the Urban Institute estimates that illegal aliens cost seven states more than $2.1 billion a year. Spending $300 million over five years to save $2 billion each year is a sound investment.

But the INS cost must be added to the SSA estimate. The Clinton Administration's latest budget request calls for $28.3 million for verification systems pilots, although this also includes other programs. The bulk of the INS cost, however, will be cleaning up their own data, which should be done regardless of the pilot projects to improve worksite verification.

- Specification of the rights, responsibilities and impact on individual workers and employers. In particular, the Commission recommendation for false negatives is that no one—no one—should be fired if their employer does not get a validation code from the registry after hiring. It is entirely possible that a new hire has merely given their Social Security Number wrong. There is no one who has a greater incentive to correct errors, whether they are at the INS or the Social Security Administration, than a legitimate worker who has just learned from the registry that there is a problem. Speaking as someone who pays into the Social Security system, I want to be sure that the number I have been using is correct—and has not been misappropriated by an illegal alien.
- A plan for phasing-in the system. Pilot projects should test various methods for phasing-in improvements in worksite verification, according to the test results.

Evaluating the results of pilot programs with these criteria must include objective measures and procedures to determine whether current problems related to fraud, discrimination and excessive paperwork requirements for employers are effectively overcome, without imposing undue costs on the government, employers, or employees.

The evaluation should pay particular attention to the effectiveness of the measures used to protect civil liberties and privacy.

While we on the Commission are not the computer experts, and never pretended to be, we do recognize "Garbage In, Garbage Out". Clearly, people who obtain real documents through false pretenses pose a problem. This is true, even though the Social Security Administration does a face-to-face interview and document check on every adult who seeks a Social Security Number, since nowadays most children receive numbers shortly after birth.

Accordingly, the Commission also recommends reducing the fraudulent access to so-called "breeder documents," particularly birth certificates, that can be used to establish an identity in this country. We recommend these steps:

- Standardized application form for birth certificates.
- Interstate and intrastate matching of birth and death records.
- Only certified copies of birth certificates issued by states should be accepted by federal agencies.
- Standard design and paperstock for all certified copies of birth certificates to reduce counterfeiting.
- Encouraging states to computerize birth records depositories.

The Commission also recommends imposition of greater penalties on those producing or selling fraudulent documents. RICO provisions to facilitate racketeering investigations should also cover conspiracy to produce and sell fraudulent documents.

The Commission's recommendations regarding worksite verification are an important part, but only a part, of a comprehensive approach to immigration reform which this Commission is developing. As you know, the Commission is well along in the next phase of its task, considering the national interest in legal immigration, including categories, priorities, and limits.

The key to our work so far has been that, through intense discussions, we have managed to arrive at a bipartisan consensus. We hope to continue that record in a systematic evaluation of what our immigration policy should be in the 21st century. In that effort, we appreciate this Subcommittee's consideration of our work.

I will be glad to answer any questions.

Mr. HORN. Thank you very much.

We will recess for 10 minutes. A quorum having been established, we will begin when we come back.

[Recess.]

Mr. HORN. The committee will come to order.

What we're going to do is wait on questioning until the whole panel is given their 5 minutes, then we will have a dialog back and forth.

Mr. Puleo, the Executive Associate Commissioner for Programs, Immigration and Naturalization Service, is accompanied by John Nahan, Director of Systematic Alien Verification for Entitlements Branch, and Gideon Epstein, Senior Forensics Analyst, Forensics Documentation Laboratory.

Gentlemen, proceed.

Mr. PULEO. Thank you, Mr. Chairman, for inviting me here today to discuss document fraud.

Improving the quality, the integrity, and the reliability of government-issued documents is critical to employer sanctions implementation and enforcement, and an important priority of the Immigration and Naturalization Service.

Until the Immigration Reform Act of 1986, it was illegal for an undocumented alien to be in the United States, but it was not illegal for an employer to hire that alien. IRCA changed the rules. It targeted employment as the single most important incentive for illegal immigration and made employers responsible for their decisions to knowingly hire unauthorized workers.

This administration is committed to the strong enforcement of employer sanctions to reduce the workplace as a magnet for illegal immigration. The President's budget request for fiscal year 1996 includes a $93-million incentive to expand current programs and to revise prior administrations' inattention to enforcement of labor standards and employer sanctions.

The administration also firmly endorses the recommendations of the Commission on Immigration Reform to conduct pilots to test various techniques for improving verification of employment authorization. These work site incentives will help to ensure that jobs are available only to authorized workers and to reduce the magnet of illegal migration.

In IRCA, Congress specified 10 documents, and by regulation INS specified 19 additional documents to be accepted by employers to verify the identity, work eligibility, or both, of newly hired employees. IRCA directs employers to accept documents presented to them that appear reasonably genuine. To counter some of the problems of the multitude of documents, the administration is preparing to test alternative verification systems on a pilot basis and to reduce the number of accepted documents.

As authorized by IRCA, INS developed and initiated the telephone verification system [TVS] pilot as a system in which employers can access the INS automated data base to confirm the employment eligibility of the newly hired noncitizens. TVS works much like a retail credit card check. The employers access the automated data base by telephone and receive an instantaneous response. If the data base lacks information or reports that the alien has no authorization, the employer mails a secondary verification to a designated local INS office.

Evaluation of phase one of TVS demonstrated it to be technically feasible and universally favorable to employers. TVS will deter fraud, since it immediately checks and verifies the INS employment status. TVS will make fraudulent documents worthless because they cannot be backed up by INS records. This, in turn, will give employers greater assurance that the employees hired and verified are truly authorized to work.

INS is expanding the TVS pilot program to 200 employers, primarily in industries that tend to attract illegal workers. TVS expansion will also involve increased safeguards to ensure that it can be implemented without discrimination or infringements on privacy.

TVS is strictly limited to noncitizens in the INS data bases. Therefore, we are working with the Social Security Administration to develop a test of a two-step process to verify all persons hired. Under this system, employers would query the Social Security Administration data base to verify Social Security numbers and check the citizenship and alien status coding of all persons hired. If the employee was an alien at the time he or she applied for a Social Security card, the employer would query the INS data base to verify employment eligibility.

We are developing a new, tamper-resistant version of the current employment authorization document, with a number of credit card-like security features. We are also centralizing card production in order to lower production costs, speed service to the public, and improve employers' ability to authenticate legitimate documents.

Finally, reducing the number of documents will reduce the opportunity for fraud and make verification simpler for employers. Therefore, within the next 30 days, INS will propose a regulation to reduce the number of acceptable documents from 29 to 16, and the administration will propose legislation further reducing the number of acceptable documents.

The INS Forensic Document Lab presently houses the largest U.S. reference collection of known and counterfeit international travel, immigration, and vital statistics documents. I would offer that any member of the committee who has not or even has visited our Forensic Document Lab to visit it anew. I think you will be quite pleased with the Forensic Document Lab.

The FDL has led the way in identification of counterfeiters and vendors of fraudulent documents by identifying their fingerprints on the documents which have been purchased through undercover operations and by linking those fingerprints to documents sold in various parts of the United States and overseas. By providing expert testimony in the major counterfeit cases, the FDL experts have strengthened our cases to an unprecedented degree, resulting in a conviction rate of major counterfeiters of more than 97 percent.

The initiatives that I have outlined represent important elements in a program to combat the problem of fraudulent documents. These steps will also considerably assist employers in complying with the employer sanctions provisions of our immigration law.

I would be pleased to answer any questions you may have. Thank you.

[The prepared statement of Mr. Puleo follows:]

PREPARED STATEMENT OF JAMES A. PULEO, EXECUTIVE ASSOCIATE COMMISSIONER FOR PROGRAMS, IMMIGRATION AND NATURALIZATION SERVICE

Thank you for inviting me here today to discuss the issue of document fraud. Improving the quality, integrity and reliability of government issued documents is critical to employer sanctions implementation and enforcement and an important priority of the Immigration and Naturalization Service (INS).

Until Congress passed the Immigration Reform and Control Act of 1986 (IRCA), it was illegal for an undocumented alien to work in the United States, but it was not illegal for an employer to hire that alien. IRCA changed the rules. It targeted employment as the single most important and pervasive incentive for illegal immigration and made employers responsible for their decision to knowingly hire unauthorized workers. It attempted to reduce the incentive of job opportunities for potential illegal immigrants and improve the conditions for all workers. This Administration is committed to strong enforcement of employer sanctions and worksite standards to reduce the workplace as a magnet for illegal immigration, while ensuring that civil rights and privacy are protected.

The President's budget request for fiscal year 1996 includes a $93 million initiative to expand current programs and to reverse prior Administrations' inattention to the enforcement of labor standards and employer sanctions. The Administration also has firmly endorsed the recommendations of the Commission on Immigration Reform to conduct pilots to test various techniques for improving verification of employment authorization and is now seeking authorization and funding to develop and implement these pilots. These worksite initiatives will help to ensure that jobs are available only to those who are authorized to work in the United States and to reduce the magnet of illegal migration.

EMPLOYMENT AUTHORIZATION VERIFICATION

In IRCA, Congress specified 8 documents and, by regulation, INS specified 21 additional documents to be accepted by employers to verify the identity, work eligibility or both of newly hired employees. IRCA directs employers to accept documents presented to them that appear reasonably genuine and relate to the person presenting them. This system has been susceptible to fraud and is confusing to some employers.

To counter some of these problems, the Administration is preparing to test alternative verification systems on a pilot basis and reduce the number of documents acceptable for establishing identity and work eligibility. While developing these pilots, the Administration is paying careful attention to privacy and discrimination issues.

TELEPHONE VERIFICATION SYSTEM (TVS) PILOT

As authorized by IRCA, INS developed and initiated the Telephone Verification System (TVS) Pilot as an alternate system for employers to confirm the employment eligibility of newly-hired employees.

INS, selected nine employers to participate in this voluntary program in which, after complying with the Form I–9 verification procedures, they can access the INS automated database to confirm the employment eligibility of the newly hired non-citizens.

TVS works much like a retail credit card check. The employers gain access to the INS automated database by telephone and receive an instantaneous response with the employees' employment authorization status. If INS lacks information or reports the employee lacks authorization, the employer mails a secondary verification to a designated local INS office. If the newly hired non-citizen's employment authorization cannot be verified through the secondary process, the employee is advised to go to the nearest INS office for possible resolution of the matter.

Evaluation of Phase I of TVS demonstrated it to be technically feasible and universally favorable by employer participants. In the first test, INS confirmed employment authorization in 70% of the cases on the basis of the initial inquiry. In the remaining cases, secondary verification took between five and ten days. Of the sample of over 2,500 cases, 99.9% were satisfactorily resolved.

TVS will deter fraud since it immediately checks and verifies with INS the employee's status. TVS will make fraudulent documents worthless because they cannot be backed up by INS records. This, in turn, will give employers greater assurance that employees hired and verified are truly authorized to work in the United States.

In 1995, INS is expanding the TVS pilot program to 200 employers primarily in industries that tend to attract illegal workers. Expansion of the TVS pilot program will also involve increased safeguards to ensure it can be implemented without discrimination or infringements on privacy. In 1996, the Administration is seeking to expand the pilot program to 1,000 employers.

The direct costs to maintain the existing status verification database which supports TVS are approximately $50,000 a year. Based on the highly favorable responses of participating employers, INS believes that these and other associated and indirect costs will willingly be borne by employers.

As we analyze and project new user requirements and workloads, we will invest in technological improvements in the secondary verification process, and improve the accuracy of the data that supports verification.

EMPLOYMENT AUTHORIZATION SYSTEM PILOTS

TVS is strictly limited to non-citizens and INS data bases. Therefore, we are working with the Social Security Administration to develop a test of a two-step process to verify all persons hired. Under this system, employers would query the SSA data base to verify Social Security numbers and check the citizenship/alien status coding of all persons hired. If the employee was an alien at the time he or she applied for the Social Security card, the employer would query the INS data base to verify employment eligibility.

This two-step pilot, which is currently in the design stage, will allow us to test the technical feasibility of verifying information on all newly-hired employees, rather than only noncitizen employees. It will also provide a test of on-line access to the SSA data base which could be a part of a future verification system.

We are also planning to simulate methods for matching INS and Social Security Administration (SSA) data to test approaches that would be restricted, secure, accurate, and nondiscriminatory. In contrast to the TVS and two-step process, electronic matching would not involve specific employees and employers.

FRAUD-RESISTANT INS DOCUMENTS AND DOCUMENT REDUCTION

An employment authorization verification system is only as sound as the validity of the documents on which it depends. Therefore, we are developing a new, tamper-resistant version of the current Employment Authorization Document (EAD) with a number of credit card-like security features including, if feasible, a magnetic stripe to permit immediate verification by an employer using a "point of sale" device. We are also centralizing card production in order to lower production costs, speed service to the public, and improve employers' ability to authenticate legitimate documents.

Finally, reducing the number of documents will reduce the opportunity for fraud and make verification simpler for employers. Therefore, within the next 30 days INS will propose a regulation to reduce the number of acceptable documents from 29 to 16 and the Administration will propose legislation further reducing the number of acceptable documents by statute.

FORENSIC DOCUMENTS LABORATORY

INS has marshaled extensive scientific and technological weapons against document fraud. The INS Forensic Document Laboratory (FDL) presently houses the largest U.S. reference collection of known and counterfeit international travel documents, immigration documents and vital statistics documents. This collection permits forensic comparison and identification of very high quality counterfeit documents and provides reference materials for training purposes. The FDL's Document Intelligence Section collects and analyzes information on current counterfeit travel documents and methods of alteration and disseminates this information in the form of high-quality color photographic document intelligence alerts to more than 200 locations throughout the United States and overseas. These alerts are the preeminent fraudulent document intelligence tool in the field.

The FDL has led the way in the identification of counterfeiters and vendors of fraudulent documents by identifying their fingerprints on documents which have been purchased through undercover operations and by linking those fingerprints to documents which have been sold in various parts of the United States and overseas. The FDL's forensic Document Link Identification System (DLIS) has made it possible to connect counterfeit document cases originating in various states to common sources and often to specific counterfeiters, thereby giving us a more accurate picture of the counterfeiting problem and identifying the origin of many of the documents sold throughout the United States.

By providing expert testimony in major counterfeiting cases, FDL experts have strengthened our cases to an unprecedented degree. This has resulted in a conviction rate of major counterfeiters of more than 97 percent once the case goes to trial. The FDL has played a major role in enforcement of employer sanctions, marriage fraud, student fraud, reentry after deportation, and the identification of criminal aliens.

CONCLUSION

We believe that the initiatives outlined to you today represent important elements in a program to combat the problem of fraudulent documents on a variety of fronts. The steps we are taking will also considerably assist employers in complying with the employer sanctions provisions of our immigration laws. These advances will enable the federal government to reduce the availability or undetected use of counterfeit documents and make the employment authorization verification process simpler and more secure.

Thank you for this opportunity to share with you INS achievements and plans in this area. I will be pleased to answer any questions.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. STEPHEN HORN TO JAMES A. PULEO

Question 1. Since the implementation of the Immigration Reform and Control Act of 1986, how many cases of immigration fraud have been referred to the U.S. Attorney's Office; how many of those have been or will be prosecuted; and what are the results (conviction, acquittal, or other) of the completed prosecutions?

Answer. The Immigration and Naturalization Service (INS) does not currently track the number of immigration fraud cases presented to the United States Attorney's Office for prosecution. However, an analysis of the Immigration Prosecution Report (G–105) revealed that from Fiscal Year 1990 through February 1995, 3,147 defendants were convicted of immigration fraud related offenses.

A review of the Performance Analysis System (G–23 report) reveals that from Fiscal Year 1990 through Fiscal Year 1994 INS Investigations completed over 4,200 criminal investigations targeting immigration document fraud facilitators and/or organizations with an income in excess of $10,000 per year from the illegal activity. At least 1,076 of these cases were developed from leads generated by employer sanctions investigations. The 4,200 cases resulted in the criminal conviction of over 1,130 defendants for immigration document fraud activity.

The Executive Office for United States Attorneys has provided the enclosed chart with figures—listed by Fiscal Year—of the immigration-related criminal fraud case disposition totals. The totals include immigration cases prosecuted under the following fraud statutes: 8 U.S.C. § 1325, 18 U.S.C. § 1001, and 18 U.S.C. § 1546.

Question 2. What were the dollar amounts requested by INS/DOJ, the amounts supported in the President's budget, and the amounts appropriated by Congress in Fiscal Years 1995 and 1996, for (1) the INS' total budget appropriation, and (2) the portions for worksite enforcement and employer sanctions?

Answer. For Fiscal Year 1995 (FY 95) the President's budget requested $1.8 billion for the INS, of which $33 million was requested for worksite enforcement enhancement. In FY 95, Congress appropriated $2 billion for the INS, of which $6 million was for worksite enforcement enhancement.

For Fiscal Year 1996 (FY 96), the President's budget requested $2.6 billion for the INS. The total request for INS worksite enforcement efforts (base funding plus enhancement) in FY 96 is estimated to be $149.9 million, of which $79.5 million is the requested enhancement. Additionally, a $2.5 million enhancement is requested for the Executive Office for Immigration Review and the Executive Office for United States Attorneys for their worksite enforcement efforts. Thus, the Department's total requested enhancement for worksite enforcement efforts is $82 million for FY 96.

Executive Office for United States Attorneys—Immigration-Related Criminal Fraud Case Disposition Totals

FY Total	Obtained Guilty Plea: Def.	Obtained Guilty Plea: Case	Trials: Def.	Trials: Case	Obtained Guilty Verdict: Def.	Obtained Guilty Verdict: Case	Acqt: Def.	Acqt: Case	Dsmissd: Def.	Dsmissd: Case
1994	366	347	8	7	5	5	3	2	35	32
1993	544	492	10	7	8	6	1	0	40	32
1992	462	403	18	16	16	14	2	2	43	35
1991	532	485	13	12	7	7	6	5	43	29
1990	616	576	6	6	6	6	0	0	45	40
1989	397	362	13	11	10	8	3	3	29	22
1988	467	420	22	13	16	8	6	5	135	92

Executive Office for United States Attorneys—Immigration-Related Criminal Fraud Case Disposition Totals—Continued

FY Total	Obtained Guilty Plea: Def.	Obtained Guilty Plea: Case	Trials: Def.	Trials: Case	Obtained Guilty Verdict: Def.	Obtained Guilty Verdict: Case	Acqt: Def.	Acqt: Case	Dsmissd: Def.	Dsmissd: Case
1987	353	316	23	20	20	18	3	2	41	28
1986	954	791	15	13	12	11	3	2	53	47

Question 3. The Automated Fingerprint Identification System (AFIS) and the Automated Fingerprint Image Reporting and Match (AFIRM) system are reportedly in use now to do Brady Act background checks for gun purchases. Is it true that the FBI is developing a more powerful and sophisticated system that will not be able to interact with either AFIS or AFIRM? If so, what greater good will offset this disturbing situation?

Answer. The INS and FBI are communicating regularly to maintain an effective partnership and exchange data concerning the status of their fingerprint system initiatives. The INS and FBI fingerprint initiatives will be able to interact with technical limitations.

The FBI is currently in the process of designing and developing a new state-of-the-art system identified as the Integrated Automated Fingerprint Identification System (IAFIS). In addition, the National Instant Check System (NICS) is being developed in accordance with the mandates set forth by the Brady Handgun Violence Prevention Act (Brady Act), and will access databases in the National Crime Information Center (NCIC) 2000 and the IAFIS. The NCIC 2000 System will provide expanded criminal justice information as well as increased functionality. The present NCIC telecommunications network is used to support interim Brady Act requirements.

IAFIS is designed to completely modernize the criminal identification services and work processes of the FBI'S Criminal Justice Information Services (CJIS) Division by providing an automated approach for performing fingerprint comparisons. The following three inter-related segments of IAFIS will work together to perform the tasks required in the processing, storage, and dissemination of criminal history records. First, the Automated Fingerprint Identification System (AFIS) will perform automated ten-print and latent fingerprint searches. AFIS will produce ranked candidate lists in response to ITN and remote search requests. Second, Identification Tasking and Networking (ITN) manages the electronic processing of fingerprint images by CJIS service providers. ITN interacts with both the III and AFIS and links networks to the FBI. Finally, the Interstate Identification Index (III) will perform automated name and biographic searches in response to ITN and NCIC requests. Upgrades to III will allow expanded criminal history record exchange.

The Department of Justice is responsible for and has tasked the FBI with the development of a NICS which will replace the five-day waiting period currently imposed under the interim provisions of the Brady Act. This system will provide users with immediate information on persons prohibited from purchasing firearms and insure the privacy and security of the NICS information. The NICS is expected to process in excess of 300,000 name check inquiries per week, including actual firearms purchases as well as concealed weapons permits, multiple purchase records inquiries, etc. This System will become operational by November 1998.

Background checks for gun purchases are currently compared against criminal history records maintained in the Interstate Identification Index (III). The NICS will be integrated with NCIC 2000 and the III segment of IAFIS to provide criminal history record information and other disqualifying data, as identified in the Brady Act, in response to background checks for firearm purchases. However, some states do submit the purchaser's fingerprints to the FBI for a more complete criminal history check than can be provided by NCIC/III alone. In addition, many states conduct a preliminary inquiry at the state level prior to making an NCIC/III inquiry.

The INS' Identification System (IDENT) is a planned biometric-based identification system and is the cornerstone of the INS biometric identification program. IDENT will assist the INS in quickly identifying persons of interest (e.g., criminal aliens and those wanted by other law enforcement agencies). Additional benefits of IDENT include improving the INS's ability to track recidivists and supporting secondary inspections at ports-of-entry. The use of this technology enables the Service to detect and prosecute criminal aliens upon apprehension.

INS also plans to apply this technology to its benefits servicing processes. Using positive identification technology to verify benefit applicants will not only ensure accuracy and integrity by tying the applicant to the proper records, but also deter claims abuse (e.g., filing separate applications under different names, imposing as the original applicant, falsifying identity information, etc.).

The differing operational requirements of the FBI's National Crime Information Center (NCIC) 2000 and the Integrated Automated Fingerprint Identification System (IAFIS) and the INS' IDENT system demand differing telecommunication media and technical characteristics to be used by the three systems.

NCIC 2000 is a rapid turnaround (seconds) inquiry/response system with a small fingerprint (FP) database, and few FP transactions per day (under 3,000) designated to accommodate operation over radio frequency networks. It will use one index fingerprint and a high degree of data compression in order to minimize interference with voice communications. NCIC 2000 is intended for missing persons and wanted fugitives whom the submitting agency can legally detain.

IDENT is a fast turnaround (seconds to a few minutes) inquiry/response system with a moderate FP size database with a high number of FP transactions per day (over 20,000). To do this it is planned to use two index fingerprints on standard telecommunication circuits. This system does not provide positive identification and must respond faster than IAFIS. The FBI IAFIS positive identification takes more time due to the human interface/interaction required within the process.

IAFIS is a moderate speed turnaround (two hours and 24 hours) positive identification system with a large FP database and a very high number of FP transactions per day (over 60,000). It will use ten fingerprints and will be designed to use high bandwidth (capacity) communications facilities. IAFIS is designed to be a complete criminal identification and history system capable of supporting crime scene investigations and positive identifications.

INS users will have the capability to use the IDENT system and its compatible fingerprint image records to access the NCIC 2000 database for fingerprint matches for warrant checks. When IAFIS becomes operational, INS will be able to electronically submit fingerprint records to the FBI's IAFIS as required and to the extent IAFIS can support the volume of civil prints.

This subject matter is extremely technical and is difficult to properly explain in lay person's terms. If you would like a fuller explanation, the FBI and INS would be happy to meet with you at your convenience.

Mr. HORN. Thank you very much. I appreciate that very thorough statement, which I read last night, and I will get to more detail in the question period.

Commissioner Shirley Chater of the Social Security Administration.

How does it feel to be independent? Do you report to anybody now that we've made you independent with an act of Congress?

Ms. CHATER. Well, actually, we're not independent for a few more days, March 31.

Mr. HORN. A few more days. I see.

Ms. CHATER. I will tell you how it feels.

Mr. HORN. Which White House assistant will you talk to?

Ms. CHATER. Could I answer that later?

Mr. HORN. OK.

STATEMENT OF SHIRLEY S. CHATER, COMMISSIONER OF SOCIAL SECURITY ADMINISTRATION

Ms. CHATER. Thank you very much for the privilege of being here to talk with you about the integrity of the Social Security card, particularly as it relates to its role in the verification of the employment eligibility process.

I do believe that my written testimony answers most of the questions and issues that you raised, sir, in your letter to us. We have just begun, as you have heard, this enormous and very complex task of developing pilot projects to test ways to strengthen the employment eligibility verification process. So some of the questions that you asked will be answered with the data that we obtain from those pilot projects.

Let me talk about the Social Security number. Verifying the number for employers is a very important function of the Social Security Administration, in that it affects accurate wage reporting as well as accurate benefit payments. Employers can call our 800 number or they can contact one of our field offices to find out what the Social Security number of a job applicant is. We can tell the employer whether a name and a Social Security number match SSA's records for that number.

Furthermore, our SSN data base is highly accurate, and I want you to know that we are proud to say that we update it every night. But that brings us, really, to the matter of what the Social Security card and the Social Security Administration cannot do. We have no way of determining, for example, whether the person presenting a Social Security card to an employer is, in fact, that person to whom the number was issued.

In terms of verifying employment eligibility, all the Social Security card can do is tell an employer whether the individual whose name is on the card has or does not have the authority to work, since the card has no features that can establish personal identification.

Now, we have taken steps to enhance the integrity of the Social Security cards and numbers. It used to be, prior to 1971, that the Social Security card was issued without any documentation at all required from the individual. However, safeguards to protect the integrity of the Social Security number issuance process were gradually put into place. Since 1978, all applicants have been required to provide documentation of age, identity, and U.S. citizenship or alien status.

We have taken some other steps over time to enhance the integrity of the card. For example, we require all applicants who are 18 years or older, and who allege that they are requesting a Social Security number for the first time, to have a personal interview. For those who say they were born in the United States, since most people born here receive a Social Security number before age 18, we perform additional verification such as checking with the State bureaus of vital statistics for birth certificates.

Another project that we have in place is called our enumeration at birth program. This allows parents in 49 States, plus the District of Columbia and Puerto Rico, to request a Social Security number for their newborn child. When they complete the form used to issue a birth certificate, the States provide SSA with the information, and SSA assigns a number and issues the card. This means that there will be fewer children without SSN's whose birth certificates could be used to obtain an SSN for another person.

Let me talk, if I might, about the card itself. We have worked hard to improve the integrity of the card. Cards are made of banknote paper and are, to the maximum extent practicable, resistant to counterfeiting. I would like to draw your attention to the cards on display, if I might. The card on the left was in use until 1983.

The card on the right, used after 1983, incorporates some of the features that I just described and, in addition, some features that I can point out to you. It has, for example, intaglio printing; that is, if you could feel the card with your fingers, you would note that the top blue band, over which "Social Security" is written, and the two columns on the card are raised, much like you feel an engraved name card.

It also has on it a sort of misty-looking marbleized blue color that would reveal an erasure, if someone tried to do that.

Third, I would draw your attention to the planchets. These are multicolored disks that are randomly placed on the face of the card. If you look very closely, you see in the lower right hand side a red one, and over to the right, a blue and a green one. These are randomly placed on the card.

Despite the improvements, however, I want us to remember that we don't expect employers to be forgery and counterfeit experts, and therefore they might, unknowingly, accept a counterfeit card.

Some have suggested that the Social Security card be enhanced with features such as a photograph, a hologram, or a magnetic strip. I would only point out what has been noted before, that were we to replace everyone's card, it would cost between $3 billion and $6 billion. And that doesn't include the cost to employers, who would have to buy equipment to read, for example, the magnetic strip on the back of the card.

We look forward to working with you, Mr. Chairman, and your committee. We look forward to our pilot projects that have already been mentioned, with the INS, because we want so very, very much to make sure that the employment eligibility for newly hired employees is as good as we can make it.

Thank you.

[The prepared statement of Ms. Chater follows:]

Prepared Statement of Shirley S. Chater, Commissioner of Social Security Administration

Mr. Chairman and Members of the Subcommittee: I am pleased to be here to discuss the integrity of the Social Security card as well as its role in the verification of employment eligibility. We look forward to working with you to address your concerns about the system.

The employment eligibility verification process is composed of two elements: verifying the identity of the job applicant and ensuring that the applicant has authority to work. SSA's role in the current work eligibility verification process is limited. A worker must present to an employer documents which establish either identity or authorization to work or both. Some documents serve as evidence of both elements, but most documents establish only one or the other. The Social Security card is in the latter category, indicating only whether the individual named on the card had authority to work when the card was issued.

For a variety of reasons which I will explain in my testimony, it is not feasible to use the current Social Security card for the purpose of establishing that the person in possession of the card is the person to whom it was issued. Perhaps no single document can guarantee identity.

HISTORY OF THE SOCIAL SECURITY CARD

Let me give you some background on the Social Security card. At the time the Social Security card was devised in the 1930's, its only purpose was to provide a record of the number that had been issued to the individual so that the employer could accurately report earnings for the individual. That is still the primary purpose for which SSA issues the card. It was never intended to serve as a personal identifier—that is, to establish that the person presenting it is actually the person whose name and Social Security number (SSN) appear on the card. Although we have made it counterfeit-resistant, it does not contain information that allows it to be used to establish identity.

Over time, however, the use of the SSN and Social Security card has greatly expanded, and the card is now used for purposes other than Social Security earnings record maintenance, including its use as evidence of authorization to work. Society's increasing use of computerized data has led to suggestions to use the SSN and the card as a personal identifier. The card itself, however, is still simply a paper record with a name and number on it.

Prior to 1971, all SSNs were issued based solely on information alleged by an individual. Because of the expanding use of the card for other purposes, there was concern about the integrity of the card. Beginning in 1971, certain categories of applicants were required to provide documentary evidence of age, identity, and alien status. This made it more difficult to obtain a card on the basis of a false identity. However, the card was still no more than a reminder of the number assigned to the individual named on the card. Because of our concern that individuals who had been assigned SSNs for purposes other than work might use the card to obtain unauthorized employment, in July 1974, we began to annotate our records to reflect the fact that an alien had been issued a nonwork SSN. This allowed us to identify, and report to the Immigration and Naturalization Service (INS), instances in which Social Security earnings were reported on nonwork SSNs.

Several years later, the integrity of the SSN process was further improved. Since May 15, 1978, all applicants have been required to provide documentary evidence of age, identity, and U.S. citizenship or alien status. Generally, to obtain an original Social Security card, an applicant must submit at least two forms of acceptable evidence, such as a birth certificate and driver's license. Aliens must submit appropriate INS documents to establish lawful status.

Any alien other than one admitted for permanent residence receives a card indicating whether he or she is authorized to work. To obtain an unrestricted Social Security card, they must provide an alien registration receipt card displaying a photograph. This document is issued to aliens by INS.

Applicants for an original SSN age 18 or over are required to have a personal interview. During the interview the applicant is asked for prior names and surnames and the reasons for never before needing an SSN. For those who allege having been born in the U.S., SSA performs additional verification prior to the issuance of an original SSN because most people born in the U.S. have been issued an SSN by the time they have reached age 18. For instance, SSA verifies the existence of a birth certificate at the State Bureau of Vital Statistics for all applicants for original cards who are over 18, and initiates a search for a death certificate when there is reason to believe the applicant may be assuming a false identity.

ENUMERATION AT BIRTH INITIATIVE

The "Enumeration at Birth" (EAB) program was established in 1989 as another means of improving the SSN process. It is a valuable tool in preventing fraudulent acquisition of an SSN. This program allows parents in the 49 participating States (plus New York City, the District of Columbia, and Puerto Rico) to indicate on the birth certificate information form whether they want an SSN issued to their newborn child. States provide SSA with birth record information about newborns whose parents want a Social Security card for their child, and SSA then assigns an SSN and issues a card. Approximately one-half of the original Social Security cards issued in fiscal year 1994 were processed through EAB. With the addition of the State of California's participation in January 1994, representing approximately 15 percent of the national births, we expect a significant increase for fiscal year 1995. This process greatly reduces the potential for someone to use another person's birth certificate to obtain a Social Security card. For example, individuals who present the birth certificate of a child enumerated under EAB would not be issued an SSN, since our records would indicate that an SSN had already been issued to the child named on the birth certificate. As EAB expands, there will be fewer children without SSNs whose birth certificates could be used to obtain an SSN for another person.

Federal income tax law requires that persons age 1 or older claimed as dependents for Federal tax deduction purposes have an SSN. By 1996, this requirement will apply to all claimed dependents. This has created a strong incentive for individuals to obtain an SSN for their children and also reduces the potential for someone else's birth certificate to be used.

We must remember that, even with these improvements to strengthen the SSN issuance process, the Social Security card is still just a record of the SSN issued and not an identity document.

GENERAL ACCOUNTING OFFICE (GAO) ANALYSIS OF ENHANCED SOCIAL SECURITY CARD

From time to time, it has been suggested that the Social Security card could be an effective proof of identity if it were enhanced. Some have proposed such features as a photograph, fingerprint or other biometric identifier, hologram, or magnetic stripe that would make the card difficult to duplicate.

GAO was directed by the Immigration Reform and Control Act of 1986 (IRCA) to look at this role for the Social Security card. GAO evaluated plastic and polyester card technologies and found that these technologies are two to ten times more expensive than paper cards. In addition, GAO noted that plastic or polyester cards wear out and have to be replaced every few years. In its March 1988 report, the GAO concluded that, even with enhancements, the Social Security card would probably not provide an effective identity system.

GAO also noted that an enhanced card would impose additional burdens on employers, yet provide no guarantee against counterfeiting. Data storage devices require the use of electronic equipment. Off-line readers would merely establish whether or not the name and SSN displayed on the card match the encoded information on the magnetic stripe. On-line systems, linked to a central data base, would be needed to both confirm the name and number match and verify the identifying data the card contains. The magnetic stripe on a plastic card is the technology most in use today. GAO reported that magnetic stripe readers cost $100-$150, a considerable outlay for many employers who would have no other use for the equipment. Also, they concluded that the commercial availability of readers and coding equipment for magnetic stripes makes this technology highly susceptible to counterfeiting. GAO also pointed out that rapid advances in card technology may quickly render obsolete any hi-tech anti-counterfeiting efforts.

Changing the Social Security card by adding a photograph and requiring that it be signed when issued might make it more effective as an identity document, but people intent on fraud can substitute a photograph, modify their appearance, or reproduce signatures with practice. In addition, pictures on the card would require updating from time to time because of changes in personal appearance.

More effective biometric identifiers, such as fingerprints, require verification techniques that are expensive and that cannot be applied by nonexperts. A technology that has emerged for linking users to documents is the Personal Identification Number or PIN. Automatic teller machines in particular have popularized this technology. However, GAO noted that incorporating a PIN in a work eligibility document would require the use of card readers and on-line access to a data base matching the PIN with a unique code in a magnetic stripe on the card. Also, GAO reported that law enforcement authorities have found that many users write their PIN on the card or elsewhere in their wallet or purse in case they should forget it. Thus, if the card is stolen, the thief also has the PIN that permits him to use the card.

GAO concluded that the card would not be a good identifier because it does not satisfy three criteria for a reliable identity document. It must be difficult to counterfeit; allow verification that the person presenting the document is, in fact, the individual to whom it was issued; and be difficult to obtain fraudulently.

We share GAO's views that these are the appropriate criteria to use in evaluating identity documents. It appears that no single document can meet all three criteria, primarily because a determined individual can obtain a counterfeit document or a valid document through fraudulent means. Furthermore, efforts to develop a fraud-proof identity document for employment eligibility verification purposes would require major changes in the process of issuing birth certificates and be very expensive. While it is possible to develop a more counterfeit-resistant Social Security card, there are reasons aside from cost-effectiveness why it would not be an effective identity document.

FALSE DOCUMENTS IMPEDE THE SECURITY OF SOCIAL SECURITY CARDS

As I mentioned earlier, even if the Social Security card were enhanced, there would be no assurance that the card had been properly issued to an individual. This is because the documents which a Social Security card applicant must present—primarily a birth certificate and immigration forms—are relatively easy to alter, counterfeit, or obtain fraudulently.

In 1988, the Office of Inspector General (OIG) of the Department of Health and Human Services (HHS) issued a report entitled Birth Certificate Fraud which examined vulnerabilities to fraud in birth certificate forms and issuance procedures and in procedures of user agencies which receive birth certificates as documentation. The problems found by the OIG included:

- False birth certificates are used to create false identities;
- An estimated 7,000 local issuing offices issue some 10,000 different versions of birth certificate forms which may be submitted to user agencies for evaluation; and,

- States have open access to vital records, and there is lax physical security of blank forms and seals, especially in local offices.

In 1991, OIG issued a follow-up report on efforts to control birth certificate fraud. The relevant finding was that the nature and extent of birth certificate fraud appeared to be relatively unchanged since 1988. OIG reported that major weaknesses in the procedures used by issuing agencies continued to hamper the ability of user agencies, both Federal and State, to rely on birth certificates as evidence of identity. The cost of revamping the system by which birth certificates are issued would be enormous, and while some State and local jurisdictions have initiated reforms, most are severely constrained from making major reforms by increasingly limited resources.

LOGISTICS OF REISSUANCE OF SOCIAL SECURITY CARDS

Let me now discuss the logistics that would be involved in issuing enhanced Social Security cards to the almost 270 million current card holders. To be effective, a new card would have to be issued relatively quickly to all card holders. Otherwise, they could present earlier versions of the Social Security card and claim they had not yet been issued a new card. The process of verifying identities and reissuing everyone a new, more secure card would be very costly—from $3 to $6 billion from general revenues, depending on the security features and issuance procedures. (The $3–$6 billion does not include the potential cost to employers.) The additional cost of the secure feature itself (e.g., a bar code or photo) would be relatively small. However, the labor costs associated with interviewing, verifying evidence, and producing the card would make the total reissuance cost extremely high.

Issuing new cards to everyone would also be burdensome on the public, as individuals would be required to establish their identity and citizenship or lawful alien status satisfactorily before being issued a new card.

The workload that would result from the issuance of new Social Security cards to all card holders would primarily serve purposes other than the administration of the Social Security program and would be a tremendous challenge for the Agency and its employees. The volume of interviews required to reissue almost 270 million Social Security cards in 5 or even in 10 years could not be handled in SSA's 1,300 local offices, because it would interfere with the ability of the offices to properly serve the people needing help with Social Security problems at a time when the Agency is facing heavy workloads. The law provides that any changes made to the Social Security card for purposes of work eligibility must be financed from general revenues and not be borne by the Social Security trust funds.

SOCIAL SECURITY CARDS FOR WORK AUTHORIZATION

I would now like to discuss the role of the Social Security card as evidence of work authorization, which is a separate issue from personal identification. As you know, Mr. Chairman, IRCA makes it illegal for an employer to knowingly hire anyone not legally permitted to work in the U.S.; that is, aliens not authorized to work by INS. Under IRCA, all employers are required to verify a job applicant's identity and authorization to work. Any of a variety of documents specified in the law and in INS regulations can be used for this verification, which is required for all employees, regardless of citizenship or national origin. Some of these documents—such as a U.S. Passport—establish both employment eligibility and identity. Others—including the Social Security card—can be used to establish work authorization, but must be accompanied by an identification document, such as a State driver's license.

Originally, the same type of Social Security card was issued to all SSN applicants who requested one, whether or not they were authorized to work. Beginning in May 1982, a legend, "NOT VALID FOR EMPLOYMENT", was placed on the Social Security cards of aliens not authorized to work to identify nonwork SSNs. This was due to the increasing need for persons to have SSNs for nonwork purposes and concern that such persons could use their SSN for work purposes. These non-employment-related Social Security cards are issued to:

- Aliens in the U.S. who do not have authorization to work, but who need SSNs for a valid nonwork purpose (such as driver's licenses in some States or bank accounts): and
- Certain aliens residing outside the U.S. (for example, dependents listed on U.S. income tax returns or individuals entitled to Social Security auxiliary or survivor's benefits).

With this legend appearing on the card, employers were able, for the first time, to determine whether an individual was authorized to work. Since September 14, 1992, cards with the legend "VALID FOR WORK ONLY WITH INS AUTHORIZATION" have been issued to aliens lawfully in the U.S. with temporary authority to work. Thus, employers are now able to determine if an alien has exceeded the time limit for his or her work authorization by checking the alien's INS document.

COUNTERFEIT-RESISTANT SOCIAL SECURITY CARDS

Originally, due to the limited purpose of the Social Security card, no special efforts were made to prevent them from being counterfeited. However, as counterfeiting became a concern, actions were taken to address this problem. For example, legislation enacted in 1983 required that new and replacement Social Security cards be made of banknote paper and—to the maximum extent practicable—be resistant to counterfeiting. The current card incorporates these and a number of other security features. It is now difficult to produce a high-quality counterfeit of these cards.

If the Social Security card were the only work eligibility document, it would have to contain features that would allow employers to easily detect counterfeit cards. Some types of humanly readable security features that make the card more counterfeit resistant are already incorporated in the current Social Security card. However, employers would have to look for them and be trained to recognize counterfeit cards. Under current law, employers are only required to make a good faith effort to ensure that documents are genuine, and they are not required to be document experts. But for the same reason that most of us will accept a counterfeit $20 bill—lack of experience and expertise in identifying a counterfeit bill—counterfeit Social Security cards may be accepted by employers.

When improved versions of Social Security cards have been developed, they have been issued only to new applicants because of the prohibitive cost of replacing all cards still in use. Thus, there are now 46 valid versions of the Social Security card in use. Approximately 61 percent of active card holders have been issued a counterfeit-resistant card. But; as I mentioned, previous versions are still valid and employers generally have no reason not to accept them.

SSA'S ROLE IN SSN VERIFICATION

It is important to keep in mind that the personal identity and Social Security card appearance issues that I have been discussing are quite separate from the issue of SSN verification. By SSN verification, we mean the process by which SSA determines whether a name and SSN match SSA's records, that is, whether SSA issued a given SSN to a given person. This process cannot determine whether the person presenting the name and SSN is, in fact, the person to whom the SSN was issued.

SSA has always had the capability to verify SSNs, which is an important function in ensuring accurate wage reporting and, ultimately, accurate benefit payments. Employers may immediately verify SSNs for payroll purposes by calling our 800-number or local office. This option is also available to employers who want to verify the SSN as part of the employment eligibility verification process. Relatively few employers call for either purpose, however, because they tend not to question the name and SSN provided by an employee. And although this option is available to employers, neither the 800 number nor local offices are equipped to handle large numbers of SSN verification requests.

With the expansion of the SSN's use over the years, especially as a result of widespread dependence on computers, SSA began to experience more and more requests for SSN verification for purposes other than the Social Security program. Many of these requests were from government agencies for the purpose of ensuring the accuracy of other Federal and State benefit programs, and automated data exchange systems were developed to comply with these requests.

On the other hand, SSA does not verify SSNs for the private sector for purposes other than employer wage reporting and employment eligibility verification. The law and our disclosure policy are designed to protect individual privacy—a fundamental and widespread concern—and the confidentiality of the SSN because of the potential for its use as a means of unauthorized access to personal records.

One of the systems that was developed to verify SSNs for States is available to employers to verify SSNs for employment eligibility verification purposes. The Enumeration Verification System (EVS), which was designed to carry out SSA's role with respect to the Federal-State Income and Eligibility Verification System (IEVS), verifies SSNs based on ASPA such as name and date of birth. Since the mid-1980's, each State has been required to have an IEVS to match financial information received from public assistance claimants with information in Federal and State data bases so that they can identify claimants who are ineligible or who receive incorrect benefit payments.

Although EVS is used primarily by States, employers may also use EVS to verify SSNs for wage reporting or employment eligibility purposes. However, because EVS consists of a high-volume process, under which the requests are transmitted to SSA by mail on magnetic tape and the results returned to the requestors in about 4 weeks, this system does not allow for immediate SSN verification. Thus, it may not effectively serve an employer's employment eligibility verification needs.

IRCA required the Secretary of Health and Human Services to study the feasibility, costs, and privacy considerations of an SSN validation system for employers. From January 1987 through September 1988, SSA tested a telephone system under which employers in 3 Texas cities requested SSN validations orally and received oral responses from SSA employees who had online access to SSA data bases. The test allowed employers to use existing telephone lines and equipment to request SSN validation of prospective employees from SSA and receive an immediate response. This is similar to an employer's calling the 800-number today, except that the test provided for a special staff dedicated to this specific function.

The test results indicated that, although technically feasible, the effectiveness of an SSN validation system in helping employers prevent aliens not authorized to work in this country from gaining employment would be limited, because there is no way to be sure that the job applicant presenting a valid Social Security card is the person to whom it was issued.

EMPLOYMENT ELIGIBILITY VERIFICATION PILOT PROJECTS

The Commission on Immigration Reform's interim report to Congress in September 1994 proposed a computer registry based on SSA and INS data which employers could check to determine if a new employee is eligible to work. The Commission recommended that the President immediately pilot the registry in the five States with the highest levels of illegal immigration and several other States.

Our SSN data base is highly accurate and is updated overnight. Since the data base was established to carry out Social Security functions, such as to facilitate wage reporting, the data base and its supporting systems are not designed to support work eligibility verification, although they contain information that is useful for that activity. Because of this, we need new programming to support verification of work eligibility and to make the verification process more convenient for employers.

The Administrtion believes that worksite enforcement of immigration laws is a necessary and effective means of controlling illegal immigration and promoting fair competition among employers and workers in the United States. The Administation's FY 1996 budget proposal includes substantial new resources to pursue this goal. As a part of this effort, the Administration is seeking to enhance effective verification of a new employee's authorization to work in the United States.

A major concern, present when Social Security started and still present today as we pursue this effort, is how best to protect people's privacy. In this age of computers and automated data banks, we must not forget the threat to personal privacy that can be posed by unauthorized access to information in government records; accordingly, we are looking at several possible measures, such as password requirements, privacy agreements with employers, and other security procedures. An Administration interagency group is also reviewing the privacy and civil rights concerns that may arise as we proceed.

On February 7, 1995, President Clinton announced several major immigration reform initiatives, including expanded worksite enforcement. To improve such enforcement, the President also anounced several pilot projects to verify employment eligibility for newly hired employees, as recomended by the Commission of Immigration Reform. The President has directed SSA and INS to develop pilot projects in response to some of the isses raised in the Commission's report and to test the feasibility of matching SSA and INS records in the future.

One of the pilot projects is a two-step process using SSA and INS data bases. Current plans call for a number of selected volunteer employers to request verification of employment eligibility by submitting to SSA a newly-hired employee's SSN, name, and a date of birth. SSA would match that information against its data base and would also cneck for citizenship/alien status coding. If SSA records indicated that the employee was an alien at the time he or she applied for an SSN card, SSA would advise the employer to verify with INS, using the employee's alien identification number, that the employee was authorized to work. We estimate that this pilot will be operational on a small scale by the end of 1995 or early 1996 in one or more geographical areas with high levels of illegal imigration. We expect to expand the pilot to more employers in 1996 and perhaps 1997.

CONCLUSION

In conclusion, Mr. Chairman, the Social Security card was originally intended to be nothing more than a means of recording the Social Security number. Its use for other purposes has provided the incentive to improve the quality of the isssuance process and the counterfeit-resistance of the card. As I have indicated, we are concerned about the possible use of the Social Security card as an identity document, the costs associated with making it serve that purpose and its implications for individual privacy; nevertheless, we are committed to testing effective, nondiscriminatory means of improving the employment eligibility verification system.

We fully undestand and share the subcommittee's concerns about improving the integrity of the employment eligibility verification system. SSA will continue to assist employers in verifying employment eligibility and we will gladly work with the subcomittee to improve that system.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. STEPHEN HORN TO SHIRLEY S. CHATER

800 Number

Question. What portion of the 800 number is paid for from trust funds and what portion from general revenues?

Answer. The 800 number is funded by SSA's Limitation on Administrative Expenses (LAE) account which is financed from the Old-Age Survivors and Disability Insurance (OASDI) trust funds, the Medicare trust funds and the general fund appropriation for the Supplemental Security Income program. Congress authorized this mix of funding in the LAE account because SSA's trust funds and SSI service delivery are so integrated. Based on the work that SSA does, the costs are allocated among the different funding sources based on a GAO approved cost accounting system. In FY 1994, about 51 percent of the SSA's administrative expenses for the LAE account was charged to the OASDI trust funds. The remaining 49 percent was charged to the Medicare trust funds (about 15 percent) and the Supplemental Security Income program (about 34 percent).

Enhanced Social Security Card

Question. Would an enhanced Social Security card be paid for from the trust funds or the general fund? Would the purpose of the enhancement make a difference?

Answer. At the time the Social Security card was devised in the 1930's, its only purpose was to provide a record of the number that had been issued to the individual so that the employer could accurately report earnings for the individual. This is still the primary purpose for which SSA issues the card.

Currently, the entire enumeration process is funded exclusively from OASDI and Medicare trust fund resources. If the purpose of enhancing the card were substantially different, the additional cost would not be a legitimate use of the Social Security trust funds and would need to be funded by a general fund appropriation.

Limitation on Administrative Expenses (LAE) Request

Question. What was SSA's LAE request for FY 1995 and what did the President request; same for 1996?

Answer. Except for technical repricing and adjustments for government-wide decisions on full-time equivalents, the Administration requested what SSA asked for in FY 1995 and FY 1996.

The President requested $5,807,174,000 and the Congress appropriated $5,540,071,000 for the LAE account for FY 1995. The President requested $6,188,200,000 for SSA's LAE account for FY 1996.

LAE and the Discretionary Caps

Question. Describe the status of limitation on Administrative Expenses (LAE) account and the discretionary caps, including which budget act imposed the caps.

Answer. The Balanced Budget and Emergency Deficit Control Act of 1985 constrains legislation that would increase spending or decrease receipts through FY 1998. It was extended and amended extensively by the Budget Enforcement Act of 1990 (BEA) and extended again by the Omnibus Budget Reconciliation Act of 1993.

In the BEA, Congress specifically exempted certain programs from the discretionary spending cap, but not SSA's administrative expenses. A subsequent exchange of correspondence between Senator James Sasser and Mr. Robert G. Darmus, Acting General Counsel, Office of Management and Budget, reaffirmed that SSA's administrative expense, including the portion funded by the Old-Age, Survivors and Disability Insurance trust funds, are subject to the discretionary spending category and BEA enforcement guidelines.

The most important thing is not whether SSA's administrative expenses are in or out of the cap, but whether SSA gets the resources it needs to get the job done.

Mr. HORN. Thank you, Commissioner. As you were talking, I happened to pull out my Social Security card, which says on the back—this is the I–46 of about 1946, really—and I notice it says on here, "For Social Security purposes, not for identification," which I gather has been dropped, because it is used, in a sense, for identification. In universities that you and I presided over, that was the basic student number.

Ms. CHATER. It is still not intended to be an identification card.

Mr. HORN. No. I know.

Ms. CHATER. And I happen to have a new one with me, and it says that it is the official verification of your Social Security number, period.

Mr. HORN. Yes. Interesting.

Well, the next panel is a person well experienced in Government, former Administrator of the Law Enforcement Assistance Administration, member of the staff of the U.S. Senate Judiciary Committee on two occasions, and an attorney-at-law in Washington, DC.

Mr. Richard W. Velde.

STATEMENT OF RICHARD W. VELDE, FORMER SENATE STAFF, ATTORNEY-AT-LAW, WASHINGTON, DC

Mr. VELDE. Thank you, Mr. Chairman.

This is a daunting task which this subcommittee faces. Having been working in these precincts for a number of years now, I'm beginning to have some appreciation of the magnitude of the problem.

My institutional memory goes back to the mid-1960's, and as a young Senate staffer, the first legislation that I worked on was what became the Gun Control Act of 1968. We were searching for a means to identify gun buyers and gun dealers. The solution at that time was to utilize, as a matter of Federal law, the State driver's license.

Indeed, the Brady Act checks, which are conducted today, are an amendment to the 1968 act. The driver's license or State identification card is still the backbone of that system. A Brady check is only as good or as bad as that driver's license.

I also became involved, in my years at the Justice Department, with the development of criminal identification and criminal history record systems, particularly automation of criminal history records. This culminated, in 1976, with the issuance of a set of regulations which govern the interstate exchange of criminal history information.

In recent years, this system has evolved so that now non-criminal-justice uses of criminal history records are more widespread than criminal justice uses. As an example, examine four pieces of recent Federal legislation, and you find common threads in all. Who cannot buy guns? Convicted felons, illegal aliens, and under age persons. Who cannot vote in most States? Most convicted felons; illegal aliens, by definition; and underage persons.

I could cite other similar pieces of Federal legislation which have similar requirements. Motor voter is another one and, of course, the recently enacted Oprah Winfrey Act, which requires criminal history background checks for all persons in child care. That's approximately 40 million people. Again, who cannot work in child care? Persons not lawfully entitled to work or live in the United

States; convicted felons, although not all; and, of course, underage persons, as well.

The problem with our identification systems in the United States is that they are literally a house of cards. They are only so good or so poor as the breeder documents upon which they are based. As was indicated here earlier and has been indicated in testimony repeatedly, throughout the last 20 years in the Congress, and as a result of a study that was conducted by the Justice Department in 1976, 4,000 agencies issue 7,000 different forms of birth certificates.

Anyone with a copy machine can reproduce many of these breeder documents. They are then the basis for Social Security cards, driver's licenses, passports, military ID cards, you name it, Federal, State, and local identification documents.

Since 1982, it has been a Federal felony offense to fraudulently misuse identification documents, as so defined. That includes Federal, State, and local documents. Since 1984, section 609(l) of the Crime Control Act of that year has established Federal standards for all identification documents: One, they shall be counterfeit-resistant; two, they shall relate positively to the identity of a particular individual. Yet we still have massive fraud.

Look at the debate on the floor of the House of Representatives last week on food stamps; where it was agreed that there was at least 10 percent fraud in that entitlement program. You look at the newspapers today, IRS is deferring refunds for 3 million individuals while detailed checks are being made on the validity of the Social Security numbers attached to those returns. According to this one press account, based on Treasury figures, at least $5 billion worth of fraud, in just this one tax refund scam at the present time.

I have here a summary of a report of the Senate Governmental Affairs Committee, its permanent Subcommittee on Investigations, until 1982, which estimates that the problem of document fraud then was $15 billion. It's probably at least $15 billion in the IRS context alone today.

Yet today, what do we have? We have the worst of both worlds. We have the onrush of technology, which makes it possible to counterfeit or reproduce very authentic-looking identification documents, and yet this technology is not being used significantly to upgrade existing identification documents so that they can meet the standards that are already a matter of Federal law.

Mr. Chairman, I have discussed these matters in my statement from a criminal justice perspective. We could just as well be talking about fraud on the passports, fraud on military ID's, fraud on all kinds of entitlement and benefit programs, not to speak of employer sanctions in the Immigration Service.

Thank you very much.

[The prepared statement of Mr. Velde follows:]

Prepared Statement of Richard W. Velde, Former Senate Staff, Attorney-At-Law, Washington, DC

Mr. Chairman and members of the Subcommittee: Existing federal, state and local identification systems have been subjected to massive fraudulent manipulation over the years. This has resulted in tens of billions of losses in various federal and state entitlement and benefit programs, as well as condoning and facilitating the presence of millions of "out of status" individuals. Many of these individuals have been a major drain on our institutions of government and taxpayers.

Although great strides have been made in the development and automation of criminal identification and information systems in the past twenty five years, much more must be done to build an integrated system that can fully take advantage of new technology. Comprehensive federal legislation is needed to allow the interstate exchange of criminal and civil sanctions must be put in place to insure the integrity of the various data bases and to protect the privacy of individuals who are the subjects of these data bases.

Existing federal law for the exchange of personal identifier information between federal, state and local authorities must be reviewed and a new comprehensive, consistent federal law enacted to enable fully the exchange of identifier information. Current law is a hodgepodge of often conflicting and technologically obsolete provisions which do not protect the privacy of affected individuals and which fall short of the standards set in the Federal False Identification Act of 1982 and the Crime Control Act of 1984.

Emergency legislation is needed to deal with endemic problems of massive fraud involving employer sanctions under the Immigration Reform Act of 1986, The Brady Handgun Violence Prevention Act of 1993, the National Child Protection Act of 1993, and The Motor Voter Act of 1994, to cite just a few of applicable federal laws which require verification of identity.

All these federal laws plus thousands of state laws and local ordinances have common characteristics:

Convicted Felons, underage individuals and illegal aliens cannot buy guns. Many convicted felons and illegal aliens cannot work in child care. Many convicted—not all—felons cannot vote. Non-citizens may not vote, nor can underage persons. Out of status persons may not live and work in the United States.

Similar prohibitions apply to various federal entitlement and benefit programs such as food stamps, education, medical and welfare.

Similar prohibitions apply in the thousands of state and local programs.

Yet all suffer from a common failing. All lack the ability to identify POSITIVELY those who are lawfully entitled to benefit from the laws; All lack the ability to identify POSITIVELY those who are to be denied the benefits of the laws.

This failure is costing us tens of billions; it robs us of job opportunities; it affects our elections; it results in increased violent crime and drug trafficking; it places heavy burdens on health care, education and housing. It contributes to passport and border crossing fraud, compromise of military identification systems and it is a massive drain on the social security system.

Our private financial and credit card industries also suffer major losses from identification fraud. All too often, they have relied on easily counterfeited or altered documents to extend credit or to provide goods and services.

Can we continue to afford this crazy quilt of conflicting and ineffective identification legislation? Just examine the congressional debate last year on health care fraud and look at the calls for a national health card. Just examine the debate on the House floor last week on food stamps and the $2–3 billion annual losses in that one program alone. Just look at the hearing records of the House Ways & Means Committee and the Senate Finance Committee over the years on fraud on the IRS. We all pay for that—but why?

The technology and the legal precedents are at hand—if only we look at the problem of identification documents in a systematic fashion and develop comprehensive legislation to regulate the interstate exchange of criminal history information. Comprehensive legislation is also needed to provide uniform national standards for identification documents. Congress has provided for uniform national standards and positive identification for commercial drivers and private pilots and aircraft owners. Why not for all drivers and others who need state identification cards?

With due respect for the Jordan Commission, there is no need for a separate national immigration data base of persons lawfully entitled to live and work in the United States to be accessed by employers under the 1986 Immigration Act.

The Commission has made a thorough investigation of the problems of document fraud and deserves high praise for its attention to this achilles heel of the employer sanctions provisions of the 1986 Immigration Reform legislation.

However, Section 101 of the 1986 Immigration Act focuses on the problem of document fraud and authorizes INS to work with state DMVs to improve the driver's license. It is laudable that INS now has a pilot program in this area—it is laughable that it has taken this long.

This information can be shared with state Motor Vehicle Departments prior to issuance of drivers licenses—on line and in real time. The Immigration Service has at least four mandates from Congress in 1986, 1988, 1990 and 1994 to share its data bases on illegal and criminal illegal aliens with state criminal justice agencies for enforcement of federal and state criminal laws. Why not make the same information available to DMVs?

These persons should not be allowed to drive as well. They should not be able to buy or make phoney IDs and other documents to rip us off and rob and steal and traffic in illicit drugs.

Then employers could begin to rely on drivers licenses as a means of positive identification for job applicants. There would be little if any need for the other 28 documents authorized by the INS for applicants to present to the employer. This amazing array makes it virtually impossible for the responsible employer to comprehend and sort out and make an informed judgement that the person applying is the person indicated on the supporting documentation. Why not concentrate on the drivers license?

EXCHANGE OF CRIMINAL HISTORY INFORMATION

In 1969 my former agency, LEAA, sponsored a demonstration effort in which a group of six state criminal identification groups came together to form a consortium called Project Search. It was charged with the task of developing a standard format for the criminal history record, or rap sheet, and then demonstrating the interstate exchange of background information. At the same time, task forces were formed to examine the questions of protection of privacy of individuals who were the subjects of the records and to insure the security of the computer systems.

Today, some 25 years later, the consortium has become a non-profit organization that includes all 50 states and federal representatives. Model state laws were formulated and are now in place in all the states, although they are far from uniform. Most repositories are automated, although millions of files are still to be converted.

In 1973 Congress authorized LEAA to issue regulations to govern the interstate exchange of the records. This was to be an interim provision to be replaced by more comprehensive legislation. In 1976, as Administrator, I issued the regulations. They are still in effect today and seem to be working reasonably well. But they are only as good as the underlying law, and do not contain a statement of national policy and priorities that should govern the exchange of rap sheet information.

In 1979, the FBI was authorized to begin a pilot project for "Triple I", the Interstate Identification Network, as part of its National Crime Information Center, for the on-line exchange of rap sheet information utilizing a "pointer" or summary system first developed in 1970 by Search Group.

BRADY GUN PURCHASER BACKGROUND CHECKS

In 1988, this authority was made permanent by the McCullom-Dole amendment on that year's crime bill, which authorized the FBI and triple I to establish a national instant system for checking the bona fides of prospective gun buyers. This provision was incorporated into the 1993 Brady Act and the states were given five years to set up the instant system. Meanwhile a national five day waiting period was instituted in those states what were not in compliance.

Today, 26 states have their own instant systems or longer waiting periods or state licensing laws. Another nine states must come into compliance before the five day waiting period is sunsetted.

The Brady Act places an affirmative mandate on chief law enforcement officers of local jurisdictions to perform background checks. In five states, led by Virginia, the state police perform the checks for dealers who are "on line" in dial up networks.

Under the 1968 Gun Control Act, eight categories of persons are prohibited from buying firearms, including convicted felons, illegal aliens and persons under 21 for a handgun and 18 for a longgun.

Unfortunately, the Brady check is a "name" check only, except for gun dealers, who must submit fingerprint cards. The name check is only good as the driver's license or "commercial" identification presented by the would be gun buyer. Without a physical or biometric verification of identity, as is contemplated in Section 609 L of the Crime Control Act of 1984, the Brady check is only as good as the paper that is presented to the dealer. The dealer should be able to determine if the drivers license is valid—that is not counterfeit, altered or expired and that the person standing there is the person to whom the license is issued.

As a general rule, state and federal(FBI) criminal history repositories do not charge for law enforcement requests for rap sheet information. However, for non-law enforcement inquiries such as employment checks various charges are made which range from a few to as much as $30. Non-law enforcement uses of criminal information systems now exceed law enforcement checks. Brady checks fall somewhere in between.

"Progun" organizations generally favor the instant check and want to see it upgraded to be more reliable and accurate. "Antigun" groups want the waiting period retained, but also support upgrade of the instant system. Congress has appropriated $100 million for implementing Brady, on top of $27 million of earmarked "Byrne" formula grants made available pursuant to the 1988 instant check legislation.

The Brady money is being used for a general program of record conversion, not just those(conviction or disposition) records that are directly relevant for compliance with the Gun Control Act requirements.

The INS should make its data bases available for Brady Act checks. Brady checks can be used by employers to determine employment eligibility just as gun dealers use the "network" through local chiefs of police(CLEOs).

The Social Security Administration should make SSN data available for these purposes as well.

A supercomputer network with five thousand terminals on line to DMVs or criminal justice agencies or employment agencies could easily handle the workload of a national employment check system. It would have a capacity with today's state of the art of supercomputer technology of handling all terminals at the same time and processing inquiries at a rate of sixty billion calculations(MFLOPS) per second.

Similar networks are already in place in the U.S. Government. This would be incredible overkill, but easily affordable and could be supported by "user fees." Or it could be linked through Internet, as is now being demonstrated by a pilot project involving the entire State of Iowa, and several cities.

The network could be decentralized or "distributed" with identifier data bases maintained at the state or local DMV installations and exchanged through NCIC, NLETS, or NDR(the National Drivers Registry of bad drivers maintained by NHSTA for background checks on commercial drivers). This network is funded at about $2 million per year(excluding state costs).

MOTOR VOTER & CHILD PROTECTION LEGISLATION

Last year Congress enacted national motor voter legislation which mandated the states to amend voting laws for federal elections so that persons who have valid drivers licenses would automatically be entitled to vote. This legislation was enacted over vigorous protests that it would lead to widespread vote fraud.

Unless Congress repeals or drastically amends this legislation, at the very least it should provide for the states to bring drivers license requirements. As with Brady checks, BEFORE a license is issued or renewed after the effective date of the federal legislation, background checks should be made to determine voting egilibility.

Who can't vote? Most convicted felons, non citizens and underage children. Who can't buy guns? The same groups. Again, the DMVs should be able to access relevant federal and state data bases to determine voter egilibility. This egilibility information should be annotated on the drivers license, in much the same way that the social security card now states whether the bearer is entitled to work.

The National Child Protection Act of 1993 requires criminal history background checks for those working the child care professions. This includes millions of workers such as teachers, day care workers and volunteers for organizations serving your people. As is the case with motor voters, who cannot work in child care? Most convicted felons, and of course, illegal aliens cannot work anywhere, including child care. Employers should have access—it need not be more than indirect—to relevant data bases for these checks.

FRAUD ON THE IRS

More than 200 million tax returns will be filed this year, with about 10 million filed electronically. This is down from 13.5 million filed last year. According to the March 6, issue of Government Computer News, the IRS intends to run electronic matching programs on SSNs on all returns. Special fraud checks are being performed on the electronic returns, especially those applying for early refunds. 3 million such returns have been held up with the prime target being the earned income tax credit(EITC).

IRS estimates that the fraud this year in this area alone might approach $5 billion.

A suit against the IRS seeking an injunction to stop the hold up was filed last week by a financial company that had many loans against the anticipated quick refunds. Documents relating to this suit will be made available to the Subcommittee for its use.

It is highly likely that many thousands of illegals have filed fraudulent claims involving the EITC, in which non-existing dependents or those residing in foreign countries have been utilized in attempting to qualify for the EITC.

The IRS is also for the first time checking on all SSNs cited in returns and running some checks on EINs as well. The problem here is compounded, however, by the fact that these are "name checks" and not physical or biometric checks based on objective identifier information, as was discussed above in relation to the Brady checks.

Again, state of the art technology must be brought to bear to upgrade electronic checks of identifier information so that a physical or biometric verification of identity can be made by IRS.

The state art in imaging and compression technology will make these physical checks in the very near future. For example, preliminary discussions have been held with respect to compressing and loading an entire state's DMV data base onto a single CD Rom disc. Then at point of contact or interaction, a live comparison can be made of the information contained in the drivers license against the CD data file and against the live "eyeball" comparison of the person standing at the counter. Search Group and the FBI have also developed fingerprint coding techniques that can serve similar verification functions by comparing fingerprint images.

Signature verification techniques can be employed such as measuring the pressure and time required to sign one's name. This can be compared against a live signature "read."

These are just three of the techniques that might be employed to upgrade name or number checks of a person's identity. I am quite confident that others will be developed in the coming months which will also make verification possible. Great strides have been made in DNA sequencing technology. In the near future, sequencing will be in real time. This will make possible the generation of a unique identifying number—15 or 50 or a 1,000 number long on each individual. It will not be intrusive. All that will be needed is a sample of hair or skin flake or spit to perform the identification. There will be no need for identification documents as we know them today. And yet identification will be positive and ultimately reliable.

Until that time comes, however, Congress and the Executive must provide leadership and courage to solve this mess we are in. Our country now faces the worst of both worlds. Modern electronic and computer technology is being used by the unscrupulous to compromise our identification systems—to copy and counterfeit and duplicate.

Yet we are not using the technology now at hand to upgrade our data bases and identity documents nor protect the privacy of our citizens. The undocumented and misdocumented still rip us off and mock our institutions and otherwise beat the system. When will we wake up and join most other advanced societies and stop this criminality? I submit, Mr. Chairman, we are long overdue.

I deeply appreciate the opportunity to testify before the subcommittee. I will submit for the record the documentation and citations for the legislation I have referred to in my testimony.

Mr. HORN. Thank you very much for that very broad perspective that you provide, having lived through and helped to recommend or draft some of the relevant laws and regulations.

Let me start the questioning and go right down the line with different questions, and then Representative Maloney and I will be sharing them in 5-minute doses, shall we say.

Mr. Hill and Ms. Martin, I'm curious, did the Commission consider a registry system or systems similar to the truck driver registry or to the Brady Act, the gun purchase one Mr. Velde mentioned, before recommending the creation of a new computerized, nationwide employment registry? And if so, what were the advantages or drawbacks of each, as the Commission saw them?

Mr. HILL. I'll let Dr. Martin answer that question.

Ms. MARTIN. Yes. The Commission did look at the other proposals for registries and the existing ones, and found the point that Mr. Velde mentioned, that most of them are contingent upon a valid Social Security number. And since the Social Security number started out as particularly connected to the employment process, it seemed that if there were, through the hiring process, a way to validate Social Security numbers through a simple, computerized system, that that then would provide the security to that number which could make these other registries work.

So we consider this to be a precondition of a number of other efforts. But basically because people use the Social Security number now when they obtain jobs, in order to have their Social Security earnings counted, that therefore seemed to be the best place to deal with the security issues up front.

Mr. HORN. Commissioner, as I understand it, the card simply shows possibly that the person holding the card has that number and that name. It doesn't really prove, conclusively, I gather, that the person is not an illegal alien, is not a felon, because they might well have doctored all their identification. But I take it, with your new systems you are checking birth certificates, which also can be fraudulent.

I just wondered what you thought of the Commission's recommendations and their comments about the Social Security system. Are you as confident as, perhaps, they are?

Ms. CHATER. It is true that the number and the name must match, and that's really all you can tell when a card is presented. I think we base the confidence in the system on the innovations that have been made to the card, making it counterfeit-resistant, while knowing that it can't be totally counterfeit-proof.

But as a result of our enumeration at birth project, for example, as time goes on, we would know that the person to whom the card was given was indeed a newborn infant. And over time that would be the way the cards were given, and we would know if anybody came forward and asked for verification of a number that had already been assigned to someone else.

Mr. HORN. If we had a single registry approach, relying primarily on Social Security, would the most sensible way be to start with those most recently issued and work our way back, in terms of base documents, be it a birth certificate, or whatever, that we could check against?

Ms. CHATER. Well, obviously, it is to our advantage, I think, to start somewhere, as long as we understand that because there are 46 styles of Social Security cards in the hands of the 270 million people who are currently active cardholders, there are always opportunities for someone to come forward with someone else's number or, indeed, the number of someone, perhaps, who has passed away, or through some other fraudulent method.

Mr. HORN. But isn't it true that most of our illegal immigrations occurred in the last two decades? So if we started with the new cards, the new checking by Social Security personnel, of having to verify birth certificates, some training, I gather from your testimony, would be needed to know the difference between likely fraudulent documents.

Ms. CHATER. Yes.

Mr. HORN. Wouldn't it make sense to start with the most recent, work our way back, replace those cards with one that we had a little more confidence in, in which not only were the number and name related, but the person behind it really was the person so named in a birth certificate somewhere in the United States, or a legal immigrant?

Ms. CHATER. Yes. You are right.

Mr. HORN. OK. When we get to that, I notice you point out that there's a difference in who pays what in the Social Security Administration. Let me ask you: Do general funds pay for that 800 number?

Ms. CHATER. Let me see. The operation of our agency comes from our administrative budget. So the answer to your question is, yes, it comes from general funds.

Mr. HORN. Now, just explain, because I think people are probably—this member is a little confused. Your administrative budget is appropriated by Congress?

Ms. CHATER. That is correct.

Mr. HORN. It is not out of the trust fund money that comes in to Social Security, now at $1 billion surplus a week?

Ms. CHATER. Let me just correct what I said to you. The 800 number, I am told, is operated partially out of the trust funds.

Mr. HORN. Out of the trust fund?

Ms. CHATER. Yes.

Mr. HORN. Now, the 65,000 employees, what funds pay them?

Ms. CHATER. Our administrative budget.

Mr. HORN. Your administrative budget appropriated by Congress?

Ms. CHATER. Some of it, because we administer the SSI program, which is paid fully by general funds. We administer the Social Security program, and those administrative expenses are funded by the trust funds.

Mr. HORN. What does that general fund budget appropriated by Congress amount to nowadays?

Ms. CHATER. For 1996, we have requested in the President's budget $6.2 billion. But I would like to also add that that's only 1.6 percent of our total budget.

Mr. HORN. Well, you've run a very efficient agency over the years, and the Congress has high respect for it. I know you are overwhelmed with a lot of things to do. But I guess what worries me is—and this becomes a philosophical question that Ways and Means would have to handle—I don't understand why, when we've got funds flowing in, why the administrative costs can't be paid out of those funds, unless they are programs that are not related to Social Security.

That's the way any other pension system would work; you would have your basic administrative expenses, and because you are so vast, it would be a fairly low percentage that is paid out of it or paid out of the investments of your funds, in Government bonds or however.

I say this because we seem to be differentiating on the cost of the card as a sort of flag waved out there saying, "Gee, it's hard for us to do it. It's $3 billion to $6 billion." Well, if we can do the 800 number out of trust funds, I don't understand why we can't replace cards out of trust funds, or we have a fee for the replacement of the card.

Ms. CHATER. As I understand it, according to the law, replacement of cards must be paid for by general funds.

Mr. HORN. OK. Well, we'll take a look at that.

Representative Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman.

I would like to ask you to respond to the possibility of unauthorized access to a data base, or even to the data base that exists now in Social Security. As you know, several years ago, employees were caught selling information, supposedly secure information, to private detectives. Have you now secured your offices for Social Security?

Ms. CHATER. We have in place a system that ensures privacy. Some of our employees, of course, have access to the data base. Each understands the penalties for misusing that data base. And when we find an employee who is suspected of having misused that data base for purposes other than Social Security purposes, we, of course, report that and follow through, because we simply must and want to protect the privacy of the data base.

Mrs. MALONEY. What happened to the two individuals that were selling the information?

Ms. CHATER. I don't know what happened to the two to whom you refer.

Mrs. MALONEY. One possible way to access any data base is by telephone, and the Jordan Commission has recommended a system that would allow employers to have access by phone to verify the eligibility of potential employees. How secure can we make a telephone verification system from unauthorized intrusions? Here in Social Security we have had examples of intrusions or misuse of information.

Mr. HILL. Certainly, that's a serious concern, Representative Maloney, one that we would like to see both the Social Security Administration and the INS address in the development of their pilot programs. But the technology, we believe, is available and it can be made to be secure, if the proper development is taken, much the way that we bank by telephone today, with PIN numbers or other forms of identification.

We think the technology will enable us to do it, but it's something that has to be worked into the pilot program so that appropriate measures are designed.

Mr. PULEO. If I may, for INS, in our telephone verification system, we download our information to a contractor so that it's kept away from the Immigration data base. The access is quite limited. We feel that the security features that we have in place are quite extensive.

Mrs. MALONEY. In Congressman Becerra's testimony he mentioned some problems that he could see and some objections he raised. And the letter that I'm sure you saw that the Hispanic Caucus sent to President Clinton raised a number of points, and I'd like to go over a few of them and have you respond to them.

Among their objections is that the pilot program is very broad in scope and is virtually the equivalent of a national system. It relies on an inaccurate Social Security and INS data base. It relies on potentially easy to forge documents, such as birth certificates and school records. And there is no obvious way for workers to prove that Social Security numbers actually belong to them.

And they claim that it would foster discrimination against U.S. citizens and legal immigrants, or any persons who might look, sound, or seem foreign.

Would you like to comment on the objections that they raised?

Mr. PULEO. I'll limit my comments to just the Immigration Service, if I can remember how they went.

With regard to the data base, I would say that it's not the inaccuracy of the data, with regard to INS, but it's in getting our data to the data base. And that's what we would hope to improve once we go to the centralized issuance of our employment authorization document from a remote process that exists in 200 separate locations throughout the United States.

By having it centralized, we will be able to download that information, at worst, the evening that the document is produced, so that the data will be timely. In fact, it would be in our data base prior to the individual receiving the employment authorization document.

We are, as I mentioned in my statement, reducing the number of documents that you can use, as an employer to verify or as an employee to gain employment, to 16. We hope to reduce that even further by regulation, or if you approve the statutory change that we are suggesting, to reduce it even further.

Mrs. MALONEY. Could I comment on that or ask a question?

Mr. PULEO. Sure.

Mrs. MALONEY. What basis do you use to select one as a better form of identification than another? What is the underlying theme or commonality that makes one document a better identification object than another?

Mr. PULEO. If you're familiar with the I–9, there are three separate columns. The first column provides both identity and authority, such as the passport, which has the photograph and is issued by the U.S. Department of State; the so-called "green card," the I–551, which INS issues to permanent residents, has a photograph, biometrics, and our current employment authorization document.

What we're looking at is, one, that it provides both authority and identity, and provides the security features that would make it fraud-resistant. There is no document that is fraud-proof. We believe, though, with improvements—and I have a mock-up here of the employment authorization document that we're going to propose—that the new document plus the data base behind it, that you would improve the authenticity of the document and the eligibility of that person to work in the United States.

Mrs. MALONEY. Thank you. My time is up.

Mr. HORN. We will be back to you.

Let me continue in a couple of other areas here. I will begin with you, Mr. Puleo.

Talking about selling documents and the fraud that occurs, we know it occurs every day in MacArthur Park in Los Angeles, on the street corners of Santa Ana. It occurs in Miami. It occurs along all the border areas.

Mrs. MALONEY. And New York.

Mr. HORN. And New York. Why can't we arrest these people and get them indicted and get them off the street?

Mr. PULEO. Well, as a matter of fact, we do. If I may, I will let Gideon Epstein give you some examples of the cases that we've recently broken and taken down.

Mr. HORN. Please. Mr. Epstein.

Mr. EPSTEIN. Yes, Mr. Chairman. Prosecutions have increased considerably in the area of fraudulent documents. There have been very large counterfeiting operations, primarily located in Los Angeles, Westminster area, where we've identified that as being the source for fraudulent documents nationwide.

There are a great many undercover operations that are presently ongoing. We've had hundreds of prosecutions. There are hundreds of individuals who have been prosecuted, and the conviction rate is extremely high in all of those cases. We do have certain rules by which we have to go. There have to be three undercover buys from a particular seller. These are laws that we have to abide by, that have been set down, before we can actually——

Mr. HORN. This is a law that we passed that says there must be three buys?

Mr. EPSTEIN. It's a procedure that has been set down.

Mr. HORN. In other words, it's the agency that sets that down, not the Congress. I can't believe we're that stupid.

Mr. EPSTEIN. I believe the U.S. attorney's offices have set that down as a policy.

Mr. HORN. The U.S. attorney's office set it down. In other words, the Congress hasn't set it down. They just said, this is a violation of the law.

Mr. PULEO. We are going to ask for changes in the sentencing guidelines to raise—limit—reduce the number of cases, with regard to sentences, to raise the sentences, reduce the number of documents you will need to produce to meet the threshold. So we are asking for changes in that.

Mr. HORN. What are the sentences? Do the judges sentence them? Are these jury cases? What happens; do we know? Are they probation, and "Good-bye; hope you're good little boys and girls?"

Mr. EPSTEIN. The major cases, those where we've actually, literally, found hundreds of thousands of documents on the premises, and where we have made the buys and then identified the cards that have been purchased against the documents that are actually found on the premises, that type of case normally results in a considerable amount of jail time.

That has gone up. It is taken much more seriously now by U.S. attorneys. In the past where some of those sentences were light, they are now becoming much stiffer, and the time served is much longer.

Mr. HORN. Well, that's good to hear, because my next question was going to be, have you had the cooperation of the U.S. attorneys in the relevant areas?

Mr. EPSTEIN. We have. Obviously, in certain areas, they have a considerable amount of crime, and it has to be sometimes a major case before they will consider it for prosecution. But I can say that in my experience with U.S. attorneys across the country in these counterfeiting cases, they are much more apt now to take these cases on and to try them, whereas a number of years ago they weren't that excited about taking them.

Mr. HORN. One of the areas this committee is looking at is the proper allocation of U.S. attorneys. We had a major hearing on that in the 103d Congress. I'd like INS to file for the record how many cases have they brought to the U.S. attorneys in this area and what has been the disposition. Which ones have the U.S. attorneys said, "Sorry, we won't go forward with them," which ones have they gone forward with, and what has been the penalty?

If they need more help, we'll be glad to try and persuade the executive branch to provide more help. And there's no question there are some complete misallocations in this country of where U.S. attorneys are. Some of the smallest States in the union have the highest number of U.S. attorneys per capita, I think, to a decision by members of the Committee on the Judiciary in the other body about 30 years ago. It's my impression they haven't changed the formula.

We would certainly welcome your help in that area, so we could be helpful in getting their attention, as needed.

Mr. PULEO. We will provide that for the record.

Mr. HORN. Very good. Now, if you could, any of you, wave a wand and say, "This is the system I'd like to have that would solve the problem we're talking about," what would you recommend?

I'd like to go down the line. What would INS like to do in this area to solve the problem?

Mr. PULEO. Well, I think it's the steps we're already taking: one, to reduce the number of documents and reduce the confusion by both the employee and the employer; improve our data base, the quantity of data that we have, not necessarily the quality; and improve the documents that we're issuing.

This is, as I said, the mock-up for the EAD, the employment authorization document, that we're looking at. We're also looking at improving the so-called "green card" to incorporate some of the state-of-the-art technology that's ongoing.

This is our automated inspections process, which takes a biometric. You may hear from other panels about incorporating a biometric in the employment authorization. I would discount that. That is not the way that we are proposing it. We were looking at that more in a controlled environment, with our permanent residents and our automated inspection process, tying this to a secure data base, which is ours.

In fact, if the employer wants to use a PC, as an example, tied into a modem, we are storing the photograph, fingerprint, and signature; you can recall that data. So if you simply swipe the magnetic stripe through a point of sale device, call up the information that's in our data base, we will in fact provide you with the photograph of the individual that should be the same photograph that's on the document.

I think reducing the confusion, a secure data base behind fraud-proof cards is the way to move it.

Mr. HORN. Mr. Hill.

Mr. HILL. The Commission's recommendations with respect to that system that you're asking are very clear. The one area that we would like to see tested, to the maximum extent possible, and to ensure flexibility, is this whole question of access by employers to that registry.

The most promising option that we see right now, based on the limited information we have, is the telephonic verification that doesn't necessarily rely on documents at all. But we recognize that it may be necessary to have a document of some sort, and that's why we have recommended testing various means of access, be it through a more secure driver's license or Social Security card. But we would be hopeful that no document, no particular document, is necessary.

Mr. HORN. Are you talking about an 800 number when you say telephonic communication?

Mr. HILL. More than likely it would be, yes.

Mr. HORN. Do you want to add anything, Dr. Martin?

Ms. MARTIN. Yes, if I could add one other element to that is that a system that doesn't rely, as Congressman Becerra was mentioning, on the self-attestation on the part of the worker, whether it's a citizen or an alien.

The current systems are really very much subject to fraud and also to the potential for discrimination, because the worker has to say, I'm a citizen or an alien. If they are an alien, there may be a possibility of an INS check, but there's nothing to stop an illegal alien from claiming to be a citizen and thereby eluding the current telephone verification process.

So we need a system which treats everybody the same way, so that employers aren't concerned that they may have somebody claiming to be a citizen who is not, so that the illegal alien can gain the system by claiming to be a citizen.

Mr. HORN. Very good. We're going to add 2 minutes to Mrs. Maloney's time. Let's finish this round.

Mr. Velde, what would you suggest?

Mr. VELDE. Mr. Chairman, we don't need a national identification system; what we need is the functional equivalent of one, which would mean the updating of State drivers' licenses and State identification documents. About half the States now, following California's lead, have digitized photographs, fingerprints, and signatures on their drivers' licenses.

In 1986, Congress passed legislation setting national standards for the testing and issuance of truck drivers' licenses. Since 1991, these images on a truck driver's license must be digitized and verifiable. That should be done for all licenses, not just truck drivers. The Federal law is already precedent for it.

Furthermore, the 13 States, such as California, that still have "open records." Those laws should be preempted by Federal Government and uniform national standards applied for the issuance of the breeder documents. Then the State identification document systems, before they are issued, such as California does—they do a 30-day background check—they should be cross-indexed with the Social Security numbers and with Immigration data bases to make sure that those individuals are lawfully entitled to live and work and drive in the United States.

Then you would have the functional equivalent of a national system at much less cost. The California driver's license now, in quantity, is under $1. It's a very durable and relatively secure document, as far as counterfeiting or alteration. There is technology available now which will allow this card to be a private credit card as well, to store enough memory on it, 2 or 4 megabytes of memory, 10,000, 20,000 pages of information, as much as you need, on the face of the card.

That's the way to go. There are many Federal laws which require the driver's license to be used as a form of identification. You cannot rely on any mail order system of issuing identification documents. That includes the passport, INS benefits, self-reporting and identification on IRS returns and forms. None require positive verification of identity, and therefore the possibilities for fraud are massive.

The driver's license or the State ID card is really the only way to go.

Mr. HORN. Thank you.

Commissioner Chater.

Ms. CHATER. I would place my confidence in the two pilot projects that are scheduled to begin very soon that were recommended as part of the Jordan Commission. And I say that because I like very much the aspect that would prevent discrimination. In other words, a potential employee going to an employer would only have to present a Social Security number instead of a raft of documents, as we now have that process in place.

This pilot, as I understand it, will require every employee to be verified, so there is initially no discrimination toward one group or another. Together with the INS and SSA working very hard on the integrity of the documents that lead to the SSN and the INS card, I think we have the potential here for doing something that's cost-effective and that doesn't trouble the employer so very much.

Mr. PULEO. Mr. Chairman, if I may.

Mr. HORN. Mr. Puleo.

Mr. PULEO. Although I don't agree in total with Mr. Velde, I do agree about the breeder documents.

One of the major problems we have, not only with employer sanctions, but to gain the other benefits of the Immigration Act, are the breeder documents; for example, the birth certificate. As Mr. Velde said, there are 4,000 entities that issue them, 7,000 different types. It's quite confusing to us, never mind the employer or anyone else. And we see them daily, those individuals claiming to be U.S. citizens by birth trying to gain benefits under the Immigration Act.

However, a secure document only goes so far. We have a folder here on a lot of counterfeit documents that were supposedly secure. So, as I mentioned, in our document, we're trying to make it counterfeit-proof, more counterfeit-proof. But without the data behind it, any document can be counterfeited, as long as you want to pay the money.

Mr. HORN. Thank you.

Mrs. Maloney.

Mrs. MALONEY. We have others.

Mr. HORN. The vice chairman has come. Which one of you was first under the rules of this committee?

Mr. Flanagan.

Mr. FLANAGAN. Thank you, Mr. Chairman.

Thank you for coming today. It's truly fascinating testimony.

Mr. Chairman, I would ask unanimous consent that I may include a statement for the record, which I will not read now.

Mr. HORN. Without objection, so ordered.

Mr. FLANAGAN. I'm deeply troubled by this, and I won't mince any words, and perhaps I'm not understanding everything that's going on. I have read, in virtually every document—and I've heard some of the testimony given today—nobody wants national identification cards. You know, we don't want people walking around with papers, having to demonstrate that they're a citizen, seemingly except in an employer context. We want to be able to tell employers that we're citizens, but not anybody else.

What slippery slope are we on? Where are we going with this? And I'm not sure I want to step out onto that line. I saw the INS collectively shake their heads. And hearing the other discussion earlier about whether we should have a State-controlled system or a national, Federal system, and everybody kind of slapped their head and said, "Well, you know, uniformity is important." Uniformity is not important.

We live in a Federalist society. We have 50 States, 50 independent laws. We have one national citizenship requirement, and to be a citizen and live and move among the several States is one requirement.

I understand the perplexing, complex—you know, that we have to deal with 7,000 different kinds of birth certificates and the difficulty of having to demonstrate our national origin to any prospective employer. I am just deeply troubled by having to carry papers, whether it includes, you know, 100 million pieces of paper of information about it or whether it's a driver's license.

I tried to get a Blockbuster card last week; they wouldn't give me one unless I gave them my Social Security card. I flatly refused. They smiled sweetly at me and said, "OK. Let's have your driver's license." I gave them that. They took the Social Security number right off of that. I found that deeply irritating. It was funny, and I laughed with them about it, but I tore up my Blockbuster card and walked out.

But the bottom line is, where are we going with a national identification card? And that's a hard question, and frank answers would be deeply appreciated. We can just start from one end and move to the other.

[The prepared statement of Hon. Michael P. Flanagan follows:]

PREPARED STATEMENT OF HON. MICHAEL P. FLANAGAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you Chairman Horn. I am very anxious to hear expert testimony today addressing the serious immigration problem in our country. Specifically, I am looking forward to understanding how we can work toward solutions, how much those solutions cost, and who pays for the solutions. Growing up in the great state of Illinois, I understand the serious problem of document fraud and how it adversely effects American citizens in their search for employment. I also am encouraged that Illinois is one of the five chosen sites for a pilot program that will produce results by 1997 that the entire country can benefit from.

Mr. PULEO. Well, as far as the Immigration Service is concerned, in 1986 Congress passed a law that made it illegal to hire illegal aliens in the United States. The sanctions are provisions of that Act. We take it extremely seriously.

We believe that there is confusion out there for both the employee and the employer. We're trying to reduce that confusion by reducing the number of documents, improving the document system that we currently have, hopefully reducing the number of documents that INS issues, too, the so-called "green card" for permanent residents and the employment authorization card for those persons here in the United States that we allow to work.

Any way we can improve the delivery of that system to make the employer sanctions provisions of the Immigration Act work better is where we, INS, are going.

Mr. HILL. Congressman Flanagan, I share your concerns about this being a very complicated issue. However, if you accept the proposition that we have a serious problem with illegal immigration in the United States—by conservative estimates approximately 4 million people in the country now illegally, approximately 300,000 added to that every year, 150,000 of which are not crossing the borders but actually coming here as visa overstayers, with legitimate, legal visas, and just simply overstaying, primarily because they find work in the United States.

If you accept that the principal magnet drawing people here illegally is jobs, then you have no alternative but to fight the problem primarily at the work site.

We looked at these issues very carefully. We are very concerned about a national ID card. We are not recommending that a card be developed that can be demanded randomly for any purpose other than the verification of employment or benefits eligibility in the United States. But the system has to be made to work. The one that we have now, the I–9 process, does not do what it was intended to do, and we need to fix it.

Mr. FLANAGAN. If I may interrupt right here. This is the "big brotherism," if I may invoke an emotional phrase into this, that was utilized since the development of the Social Security number, and having a national ID card. Now we're saying, "Well, we'll have a national ID card, but we'll only use it for this purpose." Well, you know, next year it will be this purpose and something else, and it won't be very long till it's, "Papers, please. Papers, please."

This is my concern, and I think it's a genuine one. It's one I have to explain in my district. You know, Americans are fiercely independent people, and having to demonstrate that you're a citizen to control the immigration problem is going to be a hard sell, and I think ought to be a hard sell. And I'm having trouble getting through this.

Mr. HILL. It is a difficult problem, but I don't believe that it's beyond our ability to address it through the law and through the goodwill of the people who administer that law. And I think that it is a serious problem that can be addressed and needs to be addressed, but there have to be proper safeguards instituted into the system.

Mr. VELDE. Congressman, I'll take a little different view. The United States is not nearly as far along as most other industrialized nations in having national identification systems. Just examine the American passport and the program that has been authorized now for several years, where the passport of eight other countries is recognized by the United States, so that an entry visa is not needed to come into the United States.

Not so with the U.S. passport. There have been estimates that as many as 20 percent of U.S. passports are issued fraudulently. The reason is, it's a paper transaction. There are no ways of independently verifying the identity of the applicant.

Now, there are already a number of national data bases in the United States. There are a number of highly automated, private national data bases: medical records, insurance records, educational records, and credit records. If you go to buy a car, a dealer can run a complete check on you in a few seconds.

Mr. FLANAGAN. All on a voluntary basis, though.

Mr. VELDE. All on a voluntary basis; many of them not on a voluntary basis, however, data collected without your knowledge or consent. Look, on a CD–ROM you can get a data base of every telephone number in the United States for $30. That's a national data base that has identifier information on quite a few million people.

What it is possible to do, is to build the functional equivalent of a national identification system, using State drivers' licenses or identification cards, where the data bases can be decentralized, their accuracy maintained where the people live. The driver's license has to be renewed periodically. There are many ways in which the integrity of those kinds of data bases can be maintained and secured; computer hardware and software, for example.

But we have a long way to go. As I mentioned earlier, we are paying the price here. We have the worst of both worlds. Our automation and our computer technology is being used to invade our privacy, and we don't have the benefit of a secure national system.

If you look at the exchange of criminal history information over the last 20 years, you will find safeguards in place. There is massive exchange of criminal history information, affecting the lives and the privacy and the security of many, many people. And yet we've had very little abuse of that system.

There are Federal and State laws in place that protect the privacy of individuals who are subject to these files, to ensure the quality of the data. There is biometric verification, fingerprint, now facial, now signature verification of the identity of the subject of these files. If you're going to be sentenced for an additional term of 20 years because you had three prior felony convictions, the court wants to make absolutely sure that you're that individual who had those three prior felony convictions.

So we are dealing, in the criminal justice context, with these kinds of issues all the time. Sure, there are fundamental questions of privacy and security, but now we have the worst of it.

Mr. FLANAGAN. Let me tell you, even the fact that you can safeguard that information for me does not get me over the threshold of why should you be able to collect it and then have it recorded in the first place. Whether it happens de facto or not is not reason enough for me to succumb to a national identification card, should I choose to be employed.

Mr. VELDE. Congress, in its wisdom, in the last several years has passed all this legislation: Brady checks for buying guns; motor voter; the Oprah Winfrey Act, background checks for child care employees; and employer sanctions under the immigration law.

Mr. FLANAGAN. Well, it may be too late to turn——

Mr. VELDE. You have all these Federal laws piled on top of each other requiring positive identification, and yet no means of ensuring it.

Mr. FLANAGAN. I'm not at all certain that collecting around an ability to prove who I am is the right answer. I will forego the last——

Mr. VELDE. Excuse me.

Mr. FLANAGAN. That's quite all right.

I'm sorry. Madam Director, have you a statement to make in answer to this?

Ms. CHATER. I would only add, to be sure that everyone understands, the Social Security number is not considered an identification number.

Mr. FLANAGAN. Thank you.

Thank you, Chairman, for your indulgence.

Mr. HORN. You're welcome.

Representative Maloney.

Mrs. MALONEY. Thank you. I'd like to just get back to the security and privacy. Even during Desert Storm, Dutch teenagers gained access to military computers that contained troop movement information. If the government can't protect military information, why should citizens believe that any information is secure?

And how do we balance this? I know we have a need for identification that is accurate, with securing privacy of individuals. Any of you.

Ms. MARTIN. I can begin. When the Commission looked at this issue—and shares the same concerns—where we came down to on that issue is that the ability to maintain the security of the type of registry that we've discussed is very much contingent on having a very, very select number of data items in it.

These are, basically, name, Social Security number, possibly another one or two identifiers, such as date of birth and maybe mother's maiden name, that are fairly commonly used, and then the immigration information for those, in terms of their work authorization, where it's applicable.

If that data is kept in a separate registry where the data is downloaded each night but not actually hooked back into either the Social Security data base or the INS data base, then what is in that data base is more easily securable than if you had a much larger effort. Plus, the data that's in that is not, clearly, of national security import; it's very, very basic information on name and Social Security number.

So the idea is to actually make the technology work for the privacy and security benefits rather than try to fight it, by having it as a very constrained data base.

Mr. PULEO. That's exactly what I had mentioned before, when I talked about the telephone verification system. We download limited identity information, very similar to what Dr. Martin was talking about, so that they don't have access to the entire INS data base, but sufficiently enough to either approve the employment status of the individual or, if we can't with the data we have, refer them to our offices so we can continue the process.

Mrs. MALONEY. Wouldn't a telephone verification system be incredibly expensive and labor-intensive?

Mr. PULEO. Not actually. The dollar figures that we have for not only the telephone verification system but for the SAVE system, which is another area, both held with Martin Marietta, it costs us about $700,000 a year. We estimate that just the telephone verification part of it, the cost of that is about $50,000 a year. And there's a nominal charge, I believe, for both, a transaction charge.

It's very nominal; it's not very expensive. On top of the $50,000, there's around $45,000 of INS personnel charges. So it's not that expensive. You're simply using a point of sale device that you already use for credit card verification.

Mr. Nahan is head of that.

Mr. NAHAN. Congressman Maloney, also, from the standpoint of the employers we've dealt with so far and many others who are interested, the assurance that they haven't hired someone who really was not authorized to work and who they then engage and make an investment in, with the prospect down the line that they might be removed from the payroll because they were not eligible, any little cost that they have to pay for using telephone verification is money well spent and is a very cheap proposition, in terms of the cost-benefit, from their standpoint.

But, yes, I think if you put it on a national basis, yes, there are going to be costs to run this kind of a system. No question about that.

Mrs. MALONEY. The police commissioner in New York told me there is just a huge forgery system of documents in New York City that is very sophisticated, the green card and all employment documents.

Mr. NAHAN. Well, one of the things that we think is an extremely attractive feature of our system right now, the one we're using, which is strictly a pilot—it's on a very limited basis, and it does have some limitations—but one thing that I think is its real strength is that this is the kind of system that Jim Puleo talked about that can be backed up to see if those documents aren't really, in fact, counterfeit or fraudulent.

You check them against the data base, and in almost all instances the data base is going to come back and say that's really a phony document.

Mrs. MALONEY. Thank you.

Mr. VELDE. In answer to your question, there is technology which is now becoming available, it's an offshoot of video conferencing technology and also digital compression technology, which will allow biometric verification of persons having access to computer networks. Encryption software is becoming available, so that you really have to have a verification of identity to gain access.

We all know of the hackers on Internet who are gaining access to sensitive data bases. There was a notorious hacker just arrested last week, after a nationwide search. But I think those days are limited. You will find, in the not too distant future, ability to make these data bases much more secure than we have been able to in the past.

Mrs. MALONEY. But they are not now, even to the extent of being able to enter military computers on troop movements. That's pretty scary.

Mr. VELDE. That's true. It's an evolutionary process. It's the good guys versus the bad guys, and sometimes the bad guys are ahead, and other times the good guys. And the problem is, we have such an onrush of technology, the bad guys know how to take advantage of this, as well. They are very expert now at counterfeiting just about any kind of document. But there are ways now to ensure—also by automated techniques—to ensure the integrity of these documents, and the same with these automated data bases.

Mrs. MALONEY. Is there any way that you could secure, say, the green card so that it couldn't be forged? I think a telephone system is going to be very expensive.

Mr. PULEO. We're looking at the next generation. As the next step from the employment authorization, we're looking at going to a PVC, a polyvinyl card, plastic card, as the first step of the evolutionary stage, using the EAD, then using the same platform, expanding its capabilities to produce the next generation of green cards.

You can see this is a WORM: write once, read many. The technology is very similar to your CD. This one here can hold up to 4 million bytes of memory. We're looking at something a little smaller than that. That makes it extremely expensive to counterfeit, backed up by a secure data base. So we are looking at that.

We're also looking at using similar technology for the border crossing card, which are the three major use cards INS issues. So we are looking at moving into the next century.

Mr. NAHAN. May I also make a point of clarification, and it's perhaps a problem with the way we chose to characterize. We call this a "telephone verification system," and, in fact, it does use telephone communications. But so far the only device we've used is what's called a point of sale device, which is like a credit card check. There are just a couple of pieces of information input.

There is nobody—live assistance at the other end of the line or a recorded message coming back, the way we've used this. Just like a credit card check, and it comes back with an answer very shortly.

Mrs. MALONEY. Take it to an example of someone in New York hiring someone in their home to babysit. In fact, I did that this weekend, and I asked for the green card, and I made a Xerox of it so I have my own record, and so forth and so on. But there are many small employers who don't have the Master Charge hook-up type of system. And that way I think would be very cumbersome, a telephone check, wouldn't it?

Mr. PULEO. Well, you can use an 800 number. In fact, we have it right now for a different system, our CLAIMS system, which is the automated data base where we grant benefits under the Immigration Act. You could call a number up, enter the receipt number, and an electronic voice comes back and will tell you when it was receipted, if it was approved, when it was submitted, when it was submitted or sent back to you.

So there are simple systems that you can buy off the shelf right now that can do that. When you hired the person over the weekend, you could have used an 800 number to verify that, using just your touch tone telephone.

Mrs. MALONEY. Thank you very much.

Mr. HILL. If I may, just briefly, Representative Maloney.

The example that you gave is a perfect one for one of the principal problems under the I–9 process. Under that process, the choice of documents, of course, is the employee's to give, not the employer's. Congress wrote an amendment to the law that specifically requesting any particular document is a per se violation, known as document abuse. It's one of the principal problems that employers are faced with daily, when they are concerned about the legitimacy of any particular document under the I–9 process.

Mr. VELDE. If I may allude to the gun control context, in 1988, Congress authorized a national instant background check system for purchasing a gun. Today, I can submit for the record, Mr. Chairman, a report that Treasury just issued on implementation of the Brady Act 1 year later.

There are eight States that now have instant systems in place. Virginia was the pioneer. It's a system that costs the State about $500,000 a year. Any gun dealer can simply dial up the State police, give the identifier information, and then obtain a "name" check back. You don't get positive verification of identity, but that's permissible under the Federal law.

Those systems are working reasonably well, as long as you take at face value the driver's license that is submitted by the applicant to buy the gun. I think about half the States are in compliance with Brady. Either they have their own State licensing system or some other equivalent of that. The States have until 1997 to build a national instant system.

What do you check for when you buy the gun? Whether or not you're a convicted felon, whether you're an illegal alien, whether you're underage, and five other categories. It's exactly the same check required by employers under the immigration law.

Mr. HORN. The gentleman from New Hampshire, Mr. Bass.

Mr. BASS. I have no questions at this time, Mr. Chairman.

Mr. HORN. Let me begin with a few questions, then we're going to have to break for another vote.

I noticed with interest, Commissioner, that in your statement, on page 7, you refer to the cooperation and coordination between Social Security and INS, and you say, "Since September 14, 1992, cards with the legend 'VALID FOR WORK ONLY WITH INS AUTHORIZATION' have been issued to aliens lawfully in the U.S. with temporary authority to work."

I was just curious, how many nonwork Social Security cards have received INS authorization? Have we found any gap there between what you thought, based on your records, versus what INS provided, based on their records?

Ms. CHATER. I can tell you the number of nonwork SSN's that we have counted to date.

Mr. HORN. OK.

Ms. CHATER. We have 6 million nonwork Social Security numbers at the moment.

Mr. HORN. Now, does INS have all of those people; are they knowledgeable about them?

Ms. CHATER. We report any discrepancy in our records to INS, as well as to the Inspector General's office of our department.

Mr. HORN. OK. So the Inspector General of HHS knows about this.

Ms. CHATER. That's correct.

Mr. HORN. Does INS know about that?

Mr. PULEO. Yes, we receive that information, sir.

Mr. HORN. OK. What happens to it? Do you check it against your own records so that they are similar, in the sense that these people are not to be working?

Mr. PULEO. Essentially, what the annotation says on the Social Security card is that if you, in fact, have one of these Social Security cards, you also have to have authority from the Immigration Service. So you have to show the EAD. I would say it was limited, probably, to the EAD. If, in fact, there is a discrepancy, we would check our data base to see if, in fact, the person was authorized to work here in the United States.

I can tell you, though, the likelihood of us doing an individual case is probably very remote, since we have limited resources in our investigations program. We would target—the three major priorities for our criminal investigators are: employer sanctions, fraud, and criminal aliens.

If we're doing one of our sanctions operations and it includes a large operation, if we come across this particular employee, then they will be taken down as part of that operation. But we don't have the resources to do single-issue cases.

Mr. HORN. INS has an enforcement division to watch this.

Mr. PULEO. Yes.

Mr. HORN. I'd like you to file, for the record, both Social Security and INS, over the last 2 years, what has the Commissioner of both operations asked for in enforcement funds, what has been granted by OMB, as part of the President's budget, and what has Congress provided. I'd just like that laid out for INS and the Social Security Administration.

Mr. PULEO. If I may clarify, for 1995 and 1996?

Mr. HORN. Right.

Mr. PULEO. That will be fine.

Mr. HORN. Fiscal 1995, fiscal 1996. Of course, we haven't processed the budget for fiscal 1996 yet, but at least we would have your recommendations, and then the rest is up to us, shall we say.

Mr. PULEO. Exactly.

Mr. HORN. Commissioner Chater, I'd like to know, do you have the figures on how much that 800 number really costs? I've accessed it myself, just to see if the thing worked. If you could supply the figures, we would appreciate it. They are coming out of the trust funds, and some of that is a live operator; some of that is just simply leaving name and address, if you want to make certain filings. And I assume somebody types that up and gives it to the relevant group to send the forms to the individual.

Would you say you have found the toll-free telephone line, generally, pretty successful in saving the agency a lot of time?

Ms. CHATER. Yes, it's successful. We are working very hard to make it even more successful than it is. We're trying hard to do what we call direct delivery services, so that anyone who calls our 800 number or anyone who walks into a field office will be served fully by that person, as opposed to putting them off, or telling them to come back, or even eventually making an appointment for them.

Mr. HORN. Now, with 65,000 employees, you have a lot of people, a lot of field offices spread fairly conveniently around the country. If we were to pursue making the Social Security card even more related to the individual, as the card claims to be, couldn't several thousand of your people be trained to do that out of the 65,000, and over time we could verify some of the cards? Presumably, there's what, 270 million cards out there?

Ms. CHATER. Yes. I would say that the training programs that are in place now include teaching our employees how to identify fraudulent documents. They have become sophisticated with the experience they have, but it's already part of our training program and is expected of our employees.

Mr. HORN. What I'm wondering is, if we took the approach of, work backward from the present to double-check these documents, verify the person in your area offices, couldn't we do that systematically and fairly reasonably over the next few years?

Ms. CHATER. We could certainly do it systematically, because we have verification processes in place as we speak. Large employers, for example, who want to verify the Social Security numbers of their employees, for the purposes of wage reporting—and for our purposes, for benefits, eventually—there are around 450 large employers, who send us, on a regular basis, a magnetic tape of all the employee names and numbers, so that we can verify those, find mistakes, and correct them.

We also have, as I said, our 800 number, and our field offices verify any request as to whether a name matches a number. We do that on a routine basis. Now, could we take on 6.4 million total employers and do a verification system today? I suspect the answer is no, because we are, frankly, quite stretched to the limits about what we are doing now.

And though we continue to automate and we continue to ask for funds to continue putting into place our automated system, I think we would be hard pressed to serve every employer at this moment, which is why I'm looking forward to pilot studies that will target a few, perhaps five or fewer, States, and give us some very specific cost estimates for this process to be effective.

Mr. HORN. Very good. I hate to keep you, but I'm going to have to recess for a few minutes till we cast this vote. We will be back.

[Recess.]

Mr. HORN. The committee will resume the hearing.

Let me ask you, Commissioner, what type of test does Social Security use on its accounts in a way to discover who might be using that number on a multiple basis? Some of those fraudulent numbers have to go in the books somewhere. Maybe they are even paying into the Social Security fund.

Is there a way to determine when a person is holding a—I realize we hold two jobs in this era, many people, some three jobs—but are there checks you can make to discover misuse of the number and then question it? What do you do?

Ms. CHATER. There are all sorts of ways to question the use of a number. For example, one of the new initiatives that we have in place this very year has to do with sending out a statement to people who paid into Social Security, a statement that is called the Personal Earnings and Benefit Statement, that will show people—this year everybody over the age of 60 will receive one of these in the mail.

I wrote you a letter to remind you that your constituents may be asking you questions about this, because it's a new initiative for us.

But one of the purposes of this, besides telling people what they can expect eventually and telling people what they have paid into the Social Security fund, is an opportunity for them to write to us or call us to tell us that there's a mistake, that the number isn't correct, or they have not paid in as much as we say they have, or whatever. This would cause us to look back to our records to see what the error might be, and we would make every effort to correct it.

As I indicated earlier, a second way that we check on the numbers is, when we find someone using a fraudulent number, we report that to the inspector general. If it is an INS situation, we report it there. Social Security is not an enforcement agency, so we are required by law to report these fraudulent activities to others and hope that there will be some appropriate activity taken.

Mr. HORN. Well, on that point, now you report it to the inspector general, and you present the file to the inspector general, of the investigation in question.

Ms. CHATER. Yes.

Mr. HORN. Now, what does the inspector general do with it, pursue it with the U.S. attorney, or what?

Ms. CHATER. Well, the inspector general has to make, as I understand it, some decisions about what kind of fraud to pursue. We worry, at Social Security, that they don't have enough people to pursue every incident that comes to their attention. And sometimes, if it's low on their priority list, given whatever else they have to do, it would take some time to look into it, or perhaps they choose not to look into it at all. I would have to defer to our inspector general to explain that in more detail to you.

Mr. HORN. We are going to be meeting with the inspector general, so we will pursue that.

Now, with your independence, you have your own inspector general, or have you always had that with the Social Security Administration, and not simply the HHS Inspector General?

Ms. CHATER. We have never had our own inspector general, sir. We have utilized, of course, the inspector general in the department. However, we will have our own inspector general. I have just finished interviewing, as a matter of fact, a semi-finalist list of candidates to hold the position of inspector general. We will be, next week, doing reference checks on our semi-finalists, and we're looking forward to setting up our own inspector general office.

Because we won't have an inspector general in place on March 31, we have asked—and we can do this because of the independent agency legislation—the Inspector General of the Department of Health and Human Services to continue to provide services to us, and she and I have worked out an arrangement that would focus on Social Security immediately after the 31st of March.

Mr. HORN. Is the new inspector general your appointee or the President's appointee?

Ms. CHATER. It's a Presidential appointee, but I have made it clear that I hope to be an active participant in the selection process.

Mr. HORN. I see. Very good.

Well, let me ask all of you, what question would you like to have been asked that can get something on the record that you would very much like to get on the record, that would help edify us as to what we ought to be doing in this area?

Let's go down the line. Mr. Puleo, you and your colleagues—each colleague feel free to put something on the table here. We're searching for some answers that make sense. Mr. Velde has given us a great history of this and some good suggestions as to some systems that are already in place that we might network together. I'd like to know how INS feels.

Mr. PULEO. I'm searching for a question.

Mr. HORN. Well, give me the answer, and I'll figure out the question.

Mr. PULEO. It's like Jeopardy.

Mr. HORN. That's right.

Mr. PULEO. I'm trying to recall the legislative initiative that we're working on now, with both the department and OMB, to send forward. There are some loopholes in the I–9 that we would want you to consider. The self-attestation can, in fact, give us a problem. But I'll have to pass. Other than that, I don't remember.

Mr. HORN. Well, let me just say, we're going to probably send several written questions to all of you, rather than take your time today, with other witnesses. We would appreciate it if you would answer those. You are still under oath, in terms of any followup questions from the committee.

Mr. PULEO. Absolutely.

Mr. HORN. Commissioner Hill.

Mr. HILL. Well, you've taken me a little bit off guard, but I suppose that if I wanted to get a point through on the record, I would reiterate the point that I made in my oral testimony with respect to the cost being an investment, a sound investment, and hope that the resources that are needed to do the job are fully given to the INS and the Social Security Administration so that they can do the work that's necessary to develop the infrastructure and clean up the data bases that they have to do.

Mr. HORN. Dr. Martin, would you like to add anything?

Ms. MARTIN. Only in addition to the points with regard to the infrastructure and data that Commissioner Hill mentioned, the other point that is in the written testimony, that the cost be looked at in relationship to the long-term savings that will accrue if illegal immigration is reduced; that the States and localities have been asking the Federal Government for funds to reimburse the costs of health, education, criminal justice costs, those are very high costs; and that the investment of a small amount of money up front to devise some of these systems for better verification will help save a lot of costs in the long term.

Mr. HORN. Thank you.

Mr. Velde.

Mr. VELDE. Mr. Chairman, I've already made a number of recommendations in my statement, but I would urge the subcommittee to commission a survey of Federal departments and agencies to identify and understand the number of identification systems that are in use now and try to make some sense of what the policies are, as far as who is issued, who has access, how do you maintain the security of the data bases, and so on, and hopefully obtain a comprehensive understanding of what is there.

There certainly is a desperate need for Federal legislation which establishes a uniform set of standards and policies relating to these myriad of documents that are now in use. Hopefully the Federal identification documents can be somehow integrated with those which the State and locals have.

Mr. HORN. Thank you.

Commissioner.

Ms. CHATER. I appreciated the questions that members of the subcommittee raised in regard to privacy and confidentiality, which enabled me to say to you that Social Security will do all we can to guard the confidentiality of our system and to pay attention to the privacy of the American citizen.

Mr. HORN. Representative Maloney.

Mrs. MALONEY. I would like to follow up on the comment of Dr. Martin, where you mentioned that we are now taking the steps of reimbursing localities for the high cost of medical care and the criminal justice system.

Wouldn't it be the most cost-effective and practical way just to take the first step of securing the green card, without having to take all the other steps of a telephone ID system? If that new card came into existence, that he said could not be forged, wouldn't that be a giant step forward?

Ms. MARTIN. There's a basic flaw, though, in relying only on improving the green card, and that's that there is nothing to stop an illegal alien from claiming to be a U.S. citizen, and U.S. citizens, obviously, don't have to have a green card.

What ends up happening, in that scenario, is that either the fraud works, or an employer or benefits office or anyone else who is determining eligibility of that individual, if they start second-guessing the person and saying, "Well, you have an accent, so we don't really believe you're a citizen; we want your green card," then they will be practicing discrimination against legal permanent residents and U.S. citizens who may have the appearance of being foreign.

We are very concerned about leaving it to employers to make that type of distinction. Subjective judgment as to whether or not somebody is a citizen or an alien can only lead to fraud or discrimination. That's really our concern about going down that route as the exclusive way of dealing with the problem.

Mr. PULEO. If I may, we have already taken steps to reduce the number of documents, the number of green cards, as an example. In fact, the program ends March 20 of this year, the old green card. There were 17 different versions of it.

In all the counterfeit documents that we have run across, I believe that none of them have counterfeited the most secure parts of it. If the employer is not interested in verifying—for example, we had a demonstration of simply using a black light to show the ultraviolet features of the current green card; that has never been counterfeited. An inexpensive device can verify that.

So if the employer doesn't take that step, and they are willing to take the step of verification by a telephone system, which is less costly, it appears, then you can forge parts of the document sufficiently enough to fool the employer, but unless you have massive collusion within the Immigration Service, you can't forge the data base that's behind it.

Even if we go to this card here, which I understand costs about $100 million, if you're going to try to reproduce it, it's only as good as if you want to use the security features, but the data base behind it makes it even less susceptible to fraud. And that's what we're looking at.

The EAD, for example, is less costly, but the data base behind it—and you probably may be able to forge it, if you're willing to pay the money—but the data base behind it makes it more attractive to us.

If I may, I did think of one question: These documents here are fee-based, so that if the person wants these documents, they have to pay a fee. So there's not a cost to the Immigration Service. The fee is supposed to cover the transaction of producing the documents. We have multiple sources of funding, just as Social Security does. In fact, I think we have six fee accounts, including our salaries and expense account. So these documents are fee-funded.

Mr. HORN. Before I yield to the gentleman from Illinois, let me follow up on that. As I recall, when I talked to the Commissioner about a year ago, you were exploring a number of systems. Is this essentially what you have settled on now?

Mr. PULEO. System of documents?

Mr. HORN. Right.

Mr. PULEO. Yes. We're settling on this as the employment authorization document itself and looking to use the same platform to produce the more secure green card and border crossing card.

Mr. HORN. How would you judge the fees to be? Have you thought about what you're going to set that fee at, and does it include the personnel costs involved in evaluation to grant that card?

Mr. PULEO. It's supposed to cover the entire adjudication process, which is the receipt of the document, the feeing of it—the reapplication, excuse me—the feeing of it, the adjudications of it, and the production of the card. Right now, preliminarily, these documents are not that expensive. We believe that they are still within the acceptable realm of the fee.

Mr. HORN. Are we talking $10? What are we talking about?

Mr. PULEO. I think they are less than $10. Permanent resident, this one is around $5, I believe, or $8. And then we're going down to about $2 or $3 for the other ones. We are supposed to do fee studies every year. For example, just inflation raises our fee. Every time there is a pay raise, it raises our fee because of the pay raises to the employees. It's a nominal change; sometimes, at most, it just goes up $5 a year, or $5 every time we impose a new fee.

But as we go to this, we are doing a fee study for all our fees right now. We have an independent agency coming in and doing a fee analysis for it. They will incorporate these platforms and documents in that fee study.

Mr. HORN. OK. The gentleman from Illinois, Mr. Flanagan.

Mr. FLANAGAN. Thank you, Mr. Chairman. I have just one question.

Notwithstanding our previous discussion, uncomfortable for us all though it was, Mr. Hill, I have just one question for you: Agreeing with you that, effective work site management is an effective way to deter illegal immigration, and further agreeing that we must not victimize business along the way, and understanding that we are going to make businesses a quasi-enforcement agency, to no small extent, could you briefly outline how this enforcement process would work and perhaps the penalties associated with forging documents that may be involved?

Mr. HILL. Representative Flanagan, in fact, if the verification system that we are proposing proves to be as effective and efficient as we hope it will be, the enforcement aspect of the employer's position, in fact, would decrease, because they will no longer be required to verify any particular document, its authenticity.

They will be, hopefully, in the situation of asking for one piece of information from all prospective employees, be they citizens, lawful permanent residents, or others, and that is, "What is your Social Security number?" and then verifying that through the national registry.

So it would seem to us that the employer's enforcement-related activities, if you will, would be substantially reduced under such a system, as well as the potential for fraud and counterfeit, and very important, it has been pointed out, the reduction of the potential for discrimination against legitimate American or other lawful workers, either intentionally or otherwise.

Ms. MARTIN. If I could add one aspect to it.

The Commission has also recommended that if the system works as we hope it will, that the law should be reconsidered, the employer sanctions provisions, to eliminate the penalties that employers now face for paperwork violations, for not filling out the I–9 correctly, and be focused on penalties only for knowing hire of illegal aliens and failure to verify the Social Security number, and that the ability to show that you verified the Social Security number be very simple, the confirmation numbers retailers have with the credit card companies.

So we think that that will reduce the paperwork substantially for the employers, giving them some economic advantage out of the new system. And it also will mean that INS can now put much more of its efforts into getting those who are knowingly hiring illegal aliens, who are in the underground economy, who are failing to report anything with regard to their workers and are probably violating other labor standards as well, and get off of investigating the employers who are really trying to comply with the system.

Mr. HILL. The point is, Congressman, the law already requires employers to verify the authorization to work in the United States. What we are proposing is a better system for doing that.

Mr. FLANAGAN. I understand that. I was just wondering if there were some new attendant penalties, considering the cost of having to do this.

Thank you, Mr. Chairman.

Mr. HORN. Let me follow up on that just a second.

Right now, when INS goes to an employer's office to verify, what they face in a file, I assume, is a Xerox of one's Social Security card; is that correct?

Mr. PULEO. Yes, it's usually the documents that were presented to prove that the individual can, in fact, work. If it's a Social Security card, there would also be an identity document, such as a driver's license or a State ID card, something that has a biometric on it.

Mr. HORN. Can your inspectors tell from a Xerox that that's a fraudulent card?

Mr. PULEO. It probably would be very difficult on a Social Security card, probably as difficult, maybe something less, when we start looking at our own documents, from the Xerox. It's not a requirement. We don't require the employer to do this, but they simply do it as a matter of course.

Mr. HORN. Should the employer simply hold the Social Security card as long as that person works for them?

Mr. PULEO. No. No. We don't recommend that. Plus, for example, on the green card, the alien is supposed to carry that at all times. So we would certainly not recommend that they do that.

Mr. HORN. I guess I'm thinking of European hotels, when I have to give up my American passport and feel very badly about it.

Mr. PULEO. We don't have the same enforcement authorities, nor are we seeking them, in the interior of the United States.

Mr. HILL. Mr. Chairman, may I add just one point here. The law only requires that an employer keep the actual I–9 form. They don't have to keep any supporting documentation of any kind. In fact, many large employers do not keep copies of the documents. Also, as Mr. Puleo said, the green card, for example, is also a travel document, so the employee would need that document if they were to travel out of the country.

Mr. HORN. Well, should the law say more than simply the I–9? I mean, why shouldn't you Xerox whatever they showed you?

Mr. HILL. Well, if the problem for employers that they face now is actually determining whether the document presented is an authentic document, and that is so difficult to do, it would be even more difficult to make that determination from a simple photocopy. As Mr. Puleo pointed out, it would be very difficult for INS examiners to make a determination based simply on a photocopy.

Mr. HORN. OK. Well, if there are no further questions by the panel, we thank you very much for coming and your patience between these various votes. It has been very helpful information. Thank you all.

Mr. PULEO. Thank you, Mr. Chairman.

Mr. HILL. Thank you, Mr. Chairman.

Mr. HORN. Would the panel please stand and raise their right hands.

[Witnesses sworn.]

Mr. HORN. All witnesses affirm.

All right. We will begin with Mr. Reilly unless you have decided on some order among yourselves. I'm not sure who reports to whom.

Mr. REILLY. We're all here together, Mr. Chairman.

Mr. HORN. All right. So do you want to start, Mr. Reilly?

Mr. REILLY. I'll be happy to.

Mr. HORN. Fine. Thank you.

STATEMENT OF FRANK W. REILLY, DIRECTOR, U.S. GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY HAZEL EDWARDS, DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, AND JOHN CHRIS MARTIN, ASSISTANT DIRECTOR

Mr. REILLY. Mr. Chairman and members of the subcommittee, it's a pleasure to be here today to discuss the efforts that INS and Social Security are taking to improve the integrity of data used to determine the eligibility of workers to work and receive benefits. The efforts that they are taking include assessing the feasibility of tamper-resistant cards and expanding the use of the telephone verification system.

Joining me today are two of my colleagues: Hazel Edwards on my left here, who is Director of Information Resources Management of the General Government Issues Group, and Chris Martin, who is on her left, who is the Assistant Director, responsible for security issues.

We are just going to focus on three issues, and we will touch on some of those very lightly, since you have heard so much testimony already.

We want to talk about the opportunities and limitations of the technology that INS and SSA are assessing for their systems; we want to look at how one State, Connecticut, successfully used modern technology to implement a one-step eligibility management system, which is probably fairly significant in the concerns that you are talking about here today; and finally, issues to be considered for implementing systems that are cost-effective and meet program needs.

I wanted to emphasize one thing at the beginning: In the worker identification business—because this, as you can see, is going to be a big business, however it is done—there are two universal problems of data integrity and eligibility. It is difficult to determine the real identity of the person applying for work. Frank Reilly shows up someplace for work, whether he's dark complected or whether he's light complected. To know that he is who he says he is is very difficult. Additionally, the eligibility of the person to receive the job or benefit has to be determined. These are really the two major technical issues. No matter what we talk about, it always comes back to those two points.

Now, when we talk about tamper-resistant cards, we would like to make a few comments about them. They do help reduce fraud by making it difficult to alter or duplicate the card. Various methods are available to make it tamper-resistant, and they have been talked about today. Intaglio printing, which is used in currency, and Social Security is now using this, creates that raised effect, and it's difficult to duplicate. It can be done, but it's expensive.

Another method, biometric identifiers—and I think the speaker after ourselves will talk about that—such as fingerprints that are unique to the individual cardholder. INS is developing an employment authorization card that will include a photo and a fingerprint. INS officials said this new card should help deter fraud by improving employers' ability to verify employment.

There are problems, however, with these cards. A problem with SSA use of tamper-resistant cards is the number of cards that have to be replaced, 250 million to 270 million. They have currently 44 valid versions of that, as they noted, and they noted also it will cost $3 billion to $6 billion to replace them, and that's primarily labor cost, not card stock cost. No matter how expensive the card is, the labor costs are what's going to cost all the money in that approach.

Another problem is that, while tamper-resistant cards can help improve operations, these cards alone will not ensure the integrity of employer information. People will still be able to obtain cards by using false birth certificates, as has been stressed here today, drivers' licenses, and green cards. Unless biometric identifiers are used, individuals will continue to be able to use cards that belong to others.

In our prepared statement we talked about the telephone system, and INS has gone into that in great detail, so I think that there's very little for us to say except that this kind of verification system can be useful, but it is no better than the data upon which it relies. The extent to which INS can use this verification system to determine eligibility will depend on the extent to which data in the primary data base is accurate, complete, or current.

INS has recognized that its data bases need to be improved and is initiating several actions to do so. We have submitted many reports on the problems with INS data bases. For example, it plans to interface several of its systems to allow a single point of data entry and reduce keystroke mistakes. They have a number of stovepipe systems. What they are saying is, they are going to have a single, consolidated system. That's clearly a step forward.

However, even if the INS data bases were complete and accurate, three additional problems would hinder the proper identification of illegal aliens: First, since the system is voluntary, some employers may choose not to verify their newly hired employee. Second, if employees inappropriately say they are U.S. citizens, the employer would have no reason to contact INS, since U.S. citizens are not included in the data base. And finally, illegal aliens may not be identified if they use borrowed, stolen, or forged cards of legal aliens.

Another issue, an overall technological issue that should be considered with any telephone verification, is the security and integrity of information that is transmitted over telephone lines. Depending upon the level of security desired, encryption and message authentication may be required.

Encryption is a mathematical process that transforms plain data text into ciphertext. Because this ciphertext is meaningless to an unauthorized individual, it provides confidentiality and security. One method that provides message authentication is the use of electronic signature techniques which help ensure that the data received are identical to the data that are transmitted.

The Connecticut case study is a successful use of technology by a State that has spent 4 years and about $27 million to interface with nine data bases in a totally automated system. This new system allows State employees to quickly determine an applicant's eligibility for three Federal programs and several State programs. The system has also provided greater customer service because applicants need only visit one office to be considered for benefits for all programs.

State officials reported the following productivity gains, cost savings, and benefits: They have increased the workload by 76 percent and added only 10 percent more employees. In one program alone, the number of errors decreased from 5 percent to 2.7 percent, resulting in a $10-million reduction in inappropriate expenditures. And finally, State officials identified over $5 million in attempted client fraud. So we think that system certainly paid for itself very quickly.

Finally, in conclusion, Mr. Chairman, let me emphasize three issues that must be considered: First, any system that is chosen should support program objectives. Modern technology such as tamper-resistant cards and telephone verification systems can help prevent unauthorized persons from obtaining work or other benefits. However, this technology will still be ineffective unless all other aspects of the system are also reliable. For example, the telephone verification system will be unreliable unless its related data base is reasonably accurate and complete. Likewise, tamper-resistant cards will not be effective unless accompanying controls are in place to prevent the use of stolen or duplicated cards.

A second key issue to consider is the cost-to-benefit ratio of the given system: What is it going to cost? What are you going to get out of it? No system can completely prevent fraud or abuse; thus, it is important to assess the overall risk and determine how much protection is needed to meet agency objectives. For example, on-line employer identification of worker eligibility may be too costly to implement on a nationwide basis. Depending on agency goals, implementing such a system in only those States with high immigration statistics may be sufficient.

Finally, privacy issues need to be considered when selecting technology. While integrated or shared data bases can provide valuable information, unauthorized use of this information would inappropriately infringe on the privacy of individuals.

Mr. Chairman, this concludes our prepared statement. We are willing to answer any questions you may have.

[The joint prepared statement of Mr. Reilly and Ms. Edwards follows:]

JOINT PREPARED STATEMENT OF FRANK W. REILLY, DIRECTOR, U.S. GENERAL ACCOUNTING OFFICE; AND HAZEL EDWARDS, DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION

Mr. Chairman and Members of the Subcommittee: We are pleased to be here today to discuss agency efforts to improve the integrity of data used to determine the eligibility of workers to receive benefits. Specifically, we will address efforts by the Immigration and Naturalization Service (INS) and the Social Security Administration (SSA) to address this issue.

These agencies' efforts include assessing the feasibility of tamper-resistant cards and piloting a telephone verification system. Both technologies are used to determine the eligibility of employees to work and receive benefits. As such, they are important elements in preventing individuals from illegally working and improperly receiving benefits, but they are only one part of the complete solution. Other key elements are the integrity of the data used to obtain these cards and the accuracy and reliability of the databases that support compliance activities.

Mr. Chairman, today we will focus on

- the opportunities and limitations of the technology that INS and SSA are assessing or using for their systems,
- a case study of a state that successfully used modern technology to implement a one-stop eligibility management system, and

- issues to be considered for implementing cost-effective systems that meet program needs.

OPPORTUNITIES AND LIMITATIONS OF TECHNOLOGY

INS and SSA are currently assessing several options to enhance the detection of workers who are illegally seeking employment and benefits. These options include the use of tamper-resistant identification cards and a telephone verification system. However, these technologies could be costly and they will not, taken separately, address all of the problems. For example, as we testified before the Subcommittee on Social Security and Family Policy, Senate Committee on Finance in 1990, using tamper-resistant cards will not correct the underlying condition that leads to social security card and number misuse.[1] We noted that even with tamper-resistant cards, people will still be able to obtain one or more social security numbers by using false documents, such as birth certificates or drivers licenses.

Tamper-resistant Cards

Tamper-resistant cards help to reduce fraud because they are difficult to duplicate or alter. Various methods are available to make identification cards tamper-resistant. For example, intaglio printing, such as what is used in U.S. currency, creates a raised effect in the card, making tampering difficult because the process for intaglio printing is not widely available and it is difficult to replicate.

Another method to make cards tamper-resistant is to use biometrics identifiers, such as fingerprints, that are unique to the individual card holder. INS is developing a tamper-resistant employment authorization card that includes a photo and fingerprint. INS officials stated that this new card should help deter fraud by improving employers' ability to verify employment.

A problem facing SSA as it assesses the use of tamper-resistant cards is the number of cards that will have to be replaced. SSA currently has 44 valid versions of social security number cards in use. To fully obtain the benefits of a tamper-resistant card system, SSA will have to replace all of these versions. SSA officials estimated that it will cost $3 billion to $6 billion to replace all of its active social security number cards.

Finally, as I mentioned earlier, the use of tamper-resistant cards alone will not ensure the integrity of the information, because the cards do not address all of the underlying conditions contributing to misuse. For example, people will still be able to obtain cards by using false evidentiary documents, such as birth certificates, drivers licenses, and "green cards." And, unless biometrics identifiers, such as fingerprints, are used, individuals will continue to be able to use cards belonging to others.

INS' Telephone Verification System

On March 30, 1992, INS initiated a 1-year telephone verification system pilot project to assist employers in confirming whether an alien employee is authorized to work. Nine corporations that traditionally attract large numbers of alien workers within five states (California, Florida, Illinois, New York, and Texas) volunteered and were selected to participate in this initial pilot. After hiring an individual, employers from these companies could access the verification system's database using an electronic device connected through telephone lines. Once connected, they would provide the employee's INS case file number, date of birth, and the initial of their first name. The system, in turn, would use this information to confirm the individual's employment eligibility.

INS used an extract of its central database of work authorization information as the primary verification file for the system. This extract contains over 28 million records of aliens who live in the United States. When primary verification from this file cannot be made, a secondary verification process is conducted.

This secondary process includes INS queries of other databases as well as manual searches of paper files. This secondary process, which must be completed within 10 business days from the date of the request, is much more costly and time-consuming.

INS officials told us that the employers in this pilot saw two key benefits of this system. It provided timely assurance that an alien employee is eligible for employment, and it enabled employers to minimize disruption to their business, which occurs if they have to hire and train new employees to replace employees who at a later time are identified as ineligible.

[1] Comments on S. 214—A Bill to Enhance the Integrity of the Social Security Card (GAO/T-HRD-90-23, Apr. 18, 1990).

INS considers this first pilot to be a success and is finalizing plans to expand it to include 200 employers. According to INS officials, during the first year of operation, employers verified the employment eligibility of 2,486 alien new hires—of which 72 percent were verified during the primary verification. Two hundred and thirty-six of these new hires were determined to be ineligible for employment—151 ultimately were terminated and the remainder quit work.

We agree with INS that this type of verification system has potential for helping to reduce the number of ineligible alien workers. However, such a system is no better than the data on which it relies. How much INS uses time-consuming, expensive validation efforts, such as what is needed for the secondary validation, will depend on the extent to which data in the primary database is inaccurate, incomplete, or out of date. We have reported on several occasions that INS' database is incomplete and inaccurate.[2] INS officials said they recognize that these problems continue to exist and that they are initiating several improvements. One such effort is a plan to interface several systems, which will allow a single point of data entry and reduce key stroke mistakes.

Another issue that must be considered is the security and integrity of information that is transmitted over telephone lines. Depending upon the level of security desired, encryption and message authentication may be required. Encryption is a mathematical process that transforms plain text data into ciphertext. Because this ciphertext is meaningless to an unauthorized individual, it can provide confidentiality and security. One method that provides integrity is the use of electronic signature techniques, which help ensure that data received are identical to the data that are transmitted.

Even if INS' databases were complete and accurate, three additional problems could prohibit proper identification of illegal aliens. First, the telephone verification system relies on the employer to contact INS to determine that the newly hired employee is eligible to work. Some employers may choose not to verify their newly hired employee. Second, if, on the basis of erroneous information, the employer determines the employee is a U.S. citizen, the employer would have no reason to contact INS to verify employment eligibility since U.S. citizens are not included in the database. Finally, aliens that are not legal may never be identified if they use borrowed, stolen, or forged cards of legal aliens.

Other Systems Initiatives

There are several other initiatives that SSA and INS are currently considering to improve eligibility determinations. For example, SSA and INS are looking at ways to share databases to help employers verify the work eligibility of their employees. These agencies plan to test a two-step process to cross check INS and SSA files. Each agency will access both INS and SSA databases to assist employers in verifying (1) the social security numbers and claims to U.S. citizenship and (2) work eligibility against INS files if the SSA check is not conclusive. SSA also has plans to test expanded, automated methods of providing quick-response verification of social security number cards that are used as proof of employment eligibility.

CONNECTICUT CASE STUDY—SUCCESSFUL USE OF TECHNOLOGY

Let me now focus on one state that has successfully used some of the technology mentioned above. In December 1989, Connecticut implemented an eligibility management system that improved service to both the state and its citizens. The state spent about 4 years and $27 million to totally automate its eligibility management system and interface with nine databases so that its state employees could quickly determine an applicant's eligibility for three federal programs (Aid To Families With Dependent Children, Medicaid, and Food Stamps) and several state programs.[3] With this system, applicants only need to visit one office to be considered for benefits from all these programs. A single automated file containing the complete record of the approved applicant is maintained to manage the case. In February 1995 the system had a caseload of approximately 325,000 clients.

State officials have reported the following productivity gains, cost savings, and related benefits from this automated technology:

[2] Information Management: Immigration and Naturalization Service Lacks Ready Access to Essential Data (GAO/IMTEC-90-75, Sept. 27, 1990); Criminal Aliens: Majority Deported From the New York City Area Not Listed in INS' Information Systems (GAO/GGD-87-41BR, Mar. 3, 1987).

[3] These nine databases are the Department of Motor Vehicles, Department of Labor, Bureau of Collection Services, Federal State Data Exchange, Beneficiary Data Exchange, Internal Revenue Service, Absent Parent Data, the Medicaid Management Information System, and banks.

- Productivity has increased. State officials reported they handled a 76 percent increase in cases from June 1989 to August 1994 with only about a 10 percent increase in the staff assigned to this effort.
- The number of errors has decreased, which has been accompanied by related cost savings. In fiscal year 1988, 1 year before system implementation, the Aid To Families With Dependent Children program had a reported 5.5 percent error rate of ineligible recipients and overpayments. One year after implementation, this reported error rate had declined to 2.7 percent, resulting in over a $10 million reduction in inappropriate expenditures.[4]
- The capability to identify fraud has increased. State officials have identified over $5 million in attempted client fraud.

ISSUES TO BE CONSIDERED FOR IMPLEMENTING SYSTEMS THAT MEET PROGRAM NEEDS AND ARE COST-EFFECTIVE

One of the most important considerations for any system is that it meets agency objectives for service to the public. In working toward this goal, agencies need to (1) ensure that all elements of the system support the objective and (2) compare costs against the overall objectives.

Modern technology, such as tamper-resistant cards and telephone verification systems, can help prevent unauthorized persons from obtaining work or other benefits. However, regardless of the time and money spent to make these techniques foolproof, they will be ineffective unless all other aspects of the program are also reliable. For example, the telephone verification system will not be effective unless its related database is reasonably complete and accurate. Further, tamper-resistant cards will not be effective unless accompanying controls are in place to prevent the use of stolen or duplicated authentic cards.

A second key issue to consider is the cost to benefit ratio of a given system. No system can completely prevent fraud or abuse. Thus, it is important to assess the overall risk and determine how much protection is needed to meet agency objectives. For example, on-line employer verification of worker eligibility may be too costly to implement on a nationwide basis. Depending on agency goals, implementing such a system in only those states with high immigration statistics may be sufficient.

Finally, privacy issues need to be considered when selecting technology. While integrated or shared databases can provide valuable information, unauthorized use of this information would inappropriately infringe on the privacy of individuals.

Mr. Chairman, this concludes the prepared statement. We would be pleased to answer any questions that you, or other members of the Subcommittee may have at this time.

Mr. HORN. Thank you very much. Let me ask—you were here when Mr. Velde testified, I believe, advocating utilization of the system that is already in place, which seems to have a better record of documents that actually relate to the person whose name is on the document, as opposed to Social Security and U.S. passports, where there is usually no face-to-face approach in trying to verify documents before issuing a new document.

Has the General Accounting Office any response on that particular approach as a way to solve this problem?

Mr. REILLY. Well, the use of State motor vehicle records is one of the nine data bases that Connecticut uses.

Mr. HORN. I noticed that.

Mr. REILLY. So, to the extent that you use more than a single data base, you have a lot better chance of determining whether the person in front of you is what the person purports to be. I think that's true whether we're talking about credit card systems, or identification systems, welfare systems, whatever they may be. One single system is very hard, by itself, to really ferret out all the problems.

[4] This estimated expenditure reduction was calculated by applying the reduced error rate to the 1991 expenditures.

Mr. HORN. Of those nine data bases that you list in the footnote on page 8, I believe, certainly we would agree the Department of Motor Vehicles has the best probability of relating the actual person to the name, with some evidence.

I don't know what the Department of Labor data base is. I worry about the Bureau of Collection Services, knowing so many people who have had the same name and found suddenly their credit rating was a disaster, when they had paid every bill that had ever been sent them. So that's got major problems, I would think.

I'm not sure what the Federal State data exchange is; what is that?

Mr. REILLY. There are Federal programs that are computerized and they have a data base, and they exchange this data, and the State has access to this data.

Mr. HORN. Beneficiary data exchange, what is that?

Mr. REILLY. That is the welfare beneficiary data exchange that States carry within their State and with adjoining States.

Mr. HORN. OK. We all know what Internal Revenue Service is. Absent parent data, is that the situation where——

Mr. REILLY. Child support.

Chairman HORN [continuing]. A court order has been issued in child support and somebody has ducked?

Mr. REILLY. That data base, by the way, is currently being implemented nationwide. It's due to be in this October. And the Federal Government has put about $1.2 billion into that data base alone. So, I mean, it should have a fair degree of value.

Mr. HORN. And that's based simply on absent fathers running away from responsibility?

Mr. REILLY. They get a court order and, you know———

Mr. HORN. Right.

Mr. REILLY. There's a lot of data in that.

Mr. HORN. Well, the current welfare act coming through the Ways and Means Committee will have a lot on that subject also.

And then the Medicaid Management Information System and the banks.

Mr. REILLY. Correct.

Mr. HORN. Well, the banks don't really tie photo, fingerprint, or anything to it.

Mr. REILLY. No, they do not.

Mr. HORN. So you could have a lot of flubbing in that area, as to whose account you really are.

So, when you look at it, isn't the Department of Motor Vehicles, assuming they still have face-to-face verification, face-to-face taking of the fingerprint, as well as the photo, isn't that really your best identifier?

Mr. REILLY. Well, as I say, Mr. Chairman, that is a good identifier. I mean, it can be tampered with like every other card can be.

Mr. HORN. Yes.

Mr. REILLY. If you have that together with these other ones—for example, the Medicaid Management Information System, the way Connecticut does it, they have taken the data base into their main computer file, and they use this to—they can determine the kind of medical condition that people have and are able to determine, for such things as prescriptions, whether or not they are appropriate for the people who are purporting to get the prescriptions.

Most States are going into what is known as a prospective drug utilization review system, which is intended to protect the people's health so they don't take the wrong drugs, and also intended to prevent fraud and abuse of the system.

Mr. HORN. Mr. Reilly, has GAO had an opportunity to look at the various fees that are being proposed by the Immigration and Naturalization Service and possibly the fees that might or might not be levied by the Social Security Administration for their new cards?

Mr. REILLY. I don't think we have looked at it at all, sir.

Mr. HORN. You might want to look at it. Why don't you give us your estimate as to—is there appropriate accounting? I happen to personally agree that they ought to include total transaction costs, try to pay some of the bills around here, as long as we have a $200 billion deficit. But I'd just like to know if they are on realistic ground, in terms of their cost base.

Mr. REILLY. We would be happy to.

Mr. HORN. Now, the Jordan Commission suggested the use of a personal identification number, a PIN, that a lot of us are used to on various credit cards and all the rest. Does GAO have any feeling that the PIN's help validate the process, or is biometric identification technology the only sure answer?

Mr. REILLY. Chris, do you want to answer?

Mr. HORN. Mr. Martin.

Mr. MARTIN. We talk in terms of electronic signatures, and I think it's important that I define that term. It is used by a lot of people who say, "I have electronic signatures," and don't. GAO has issued the criteria that we use in assessing systems or electronic signature systems in financial management and procurement applications. That authority is granted to us under Title XXXI of the United States Code.

In December 1991, we issued a Comptroller General decision (71 Comp. Gen. 109), and we have also issued several reports that outline that criteria. The three criteria we use are that a signature, whether it's handwritten, electronic, or otherwise, auto-pen—you can go through any number of systems—has to meet the following three criteria: One, it has to be unique to the signer; two, it has to be under the signer's sole control; three, it has to be capable of being verified.

In addition, to evidence the signer's intent, the signature has to be linked to the data in such a manner that, if the data is changed, the signature is invalidated. This is consistent with the way that we view a paper document. It's no different, the criteria for electronic. We aren't asserting anything for electronic signature that is different than a paper document.

GAO has sanctioned the operation of two electronic signature systems and is monitoring the development of two others, at the request of the agencies. We have not reviewed systems the private sector is using. Probably one that you are familiar with, that you can see on TV, is that some delivery systems come up and have you sign a board.

We haven't reviewed those, but we have reviewed technology that is very similar to that. That is not what we would consider an electronic signature. Specifically, the data in that system is not linked to that signature. All I need is that digitized image and I can attach it to any data record and, in effect, "forge" that record.

If you think of it in the paper world, it's much like if we had a class here and I asked everybody to sign to show that signatures are different, and somebody goes to the trash can and picks it up and then attaches that piece of paper to a mortgage document and says, "You signed a mortgage for $1 million." There's not a link there between the signature and the data, so it doesn't hold up. That's why we use those four criteria in our systems.

Mr. HORN. Very interesting.

Would you like to add something, Ms. Edwards?

Ms. EDWARDS. On the subject of biometrics versus a PIN, there are a couple of thoughts to hold in mind. One is that biometrics are unique identifiers, such as your fingerprint, that would certainly uniquely distinguish one person from another. With a PIN number, as you know, it's a series of digits that people remember, or frequently, more than likely, write it down on a piece of paper. So one is far more transferable than the other.

With regard to the use of a biometric versus a PIN, if the costs were not a consideration, I think the preference would be for a biometric, something that would uniquely identify an individual. The application that's chosen by an agency will determine which one is most appropriate and cost-effective—whether the agency should choose a PIN type structure or whether they should employ a biometric.

Mr. MARTIN. There are weaknesses with PIN's. If you think of your bank card, most of those are four digits. That means there are only 9,999 possibilities. You were talking earlier about the hackers. If that PIN is transmitted over unsecured lines, a person can pick up that PIN.

The same danger runs in biometrics. If, for example, I have my fingerprint and I am here, and it takes a reading, and it's sending it clear across lines, there again, all I need to do is capture that digitized image and I can masquerade as you, or you can masquerade as me.

That's why you need to link the data and the signature together in such a manner that if one of them is changed, you know that you have a problem.

Mr. HORN. Interesting.

Representative Maloney.

Mrs. MALONEY. The Urban Institute estimated that 86 percent of the illegal aliens are in five States. What is the cost-benefit ratio for expanding the system nationwide to capture the last 14 percent?

Mr. REILLY. I would ask the same question. I would absolutely ask the same question. I think that's a very valid question.

Mrs. MALONEY. Well, if you instituted or set up a system in just five States, do you think that then the problem would jump over to other States?

Mr. REILLY. Well, you know, we're dealing with a cost-benefit analysis. And if, as you said, 86 percent are in five States, then I think you've got—I mean, unless there are some other facts that we don't know, I think you would certainly want to start with those five States.

I think those five States, if they have 86 percent of the population that you're trying to deal with, that's certainly the place you would begin. And if you find it really works well there, then I think you would move someplace else. But I couldn't raise any disagreement with what you said.

Mrs. MALONEY. Do you believe you can protect privacy with a national ID system?

Mr. REILLY. I think protecting privacy is going to become one of the most critical issues for the Congress—and I don't know whether this Congress or subsequent—because it isn't just these cards, Social Security and INS, we're all going to be—in a few years, everybody is going to have computerized medical records. And there's probably nothing more private than a person's medical record.

And we're going to have to have this because, if we have an emergency room and somebody shows up in an emergency room, and we have all the capability in the country to have people's records computerized, then you are certainly going to want to have that information to be available in that emergency room, when you show up, and you're unconscious and they want to take care of you, and they need that kind of information.

So this is going to become a real issue, in terms of our health and our longevity and the ability of doctors to take care of us properly, going from one HMO to another, going from one doctor to another. So we know that coming down the road these kinds of technologies are in the marketplace and are being developed.

So this privacy issue is not just related to INS and Social Security; it's going to be related to technology. And I think it can be dealt with, and I think that ultimately it will be dealt with.

Mrs. MALONEY. Well, how do you deal with it?

Mr. REILLY. The last Congress had a number of bipartisan supporters of a privacy law, in both the House and Senate, and unfortunately it was not able, at the last moment, to get attached to a piece of legislation. But my understanding is, this legislation was quite complete and it dealt with all of the various kinds of privacy issues. And I don't know where the legislation stands now, but I think that might be a good place to begin.

Mrs. MALONEY. Thank you very much.

Mr. HORN. The gentleman from Virginia, Mr. Davis.

Mr. DAVIS. Thank you, Mr. Chairman. I apologize for not being here. I had another subcommittee meeting today.

I think you talked about the INS problem of the disparate computer data bases. How long is it going to take and what level of resources will it take to overcome the problem? What are the budget implications? Any thoughts on that?

Mr. REILLY. Mr. Davis, before you were here, the people from INS and Social Security, they had extensive discussions on this, and I did not hear a definitive answer on what it was going to cost or how long it was going to take.

What they are working on now are pilot tests. They currently have nine employers, and they were talking about what it would cost for the nine employers, but what it would cost to do the five

States, for example, that have 86 percent of the workload, those kinds of details were not provided. So I really can't tell you.

Mr. DAVIS. OK. Thank you. That's all.

Mr. HORN. We just asked GAO to check out their possible fee schedule, which would include, as maybe you heard me say, the total transaction costs and labor costs as well.

Let me ask here, your assessment in response to Mrs. Maloney, it seems to me that while 86 percent of the illegal problem is in five States, if you concentrate on those States, it's like chasing gangs in one city; they just go to the next city. And you will simply be spilling over into other States.

The fact is, illegals are in every State. They are spread around the country. We don't talk about the northern invasion across the Canadian border as much as the southern invasion, or the Atlantic and Pacific invasions. The Congress finally awakened 2 years ago when you had boats of Chinese crammed full, waiting to land in the Pacific Coast and the East Coast. That finally woke most people up here who hadn't done much or cared much, frankly, about illegal immigration.

I'd like to think the argument I made that they lost a number of seats to California in the 1990 census also woke them up. We went from 45 to 52, and of those roughly 7 seats, I think probably 4 or 5 are due to our illegal alien population in that decade, because they count as persons under the census. Pennsylvania lost 2. Kentucky lost 1, et cetera. That will happen again in the year 2000 if we don't solve the problem.

Now, has GAO gone in and looked at the total cost of illegal aliens to this country? Have you ever done a study on this? The Urban Institute has looked at one aspect, the cost of alien prisoners. As I remember, their figure is something like—in California, it would be $250 million; whereas, the Governor says it's $350 million, this kind of discrepancy for the 20,000 or so illegal alien prisoners we incarcerate in California, in the State prison system.

Mr. REILLY. Have we? Ms. Edwards.

Ms. EDWARDS. We have not conducted any independent analyses in those areas. As you point out, the Urban Institute has done some work. But at the base of all of the analyses is the lack of sufficient and specific data.

What we have done is look at the basis upon which the Urban Institute study was conducted and essentially came to the conclusion that we can't make a decision one way or another as to the goodness of the numbers, given that the data was so skimpy, aside from the incarceration data, which is easier to track.

On a separate front, we are continuing to look at other studies, and I think there is some work presently underway at GAO to look at other studies which attempt to quantify the expenses associated with the illegal alien population. But the extent of our work has been to review other independent studies.

Mr. REILLY. Mr. Chairman, if I may, my response to Congresswoman Maloney is, the problem that we constantly run into in technology is the cost of it. I mean, everybody has raised that issue today. What we're saying is that if we're going to do pilot tests, it would certainly be the place to do it in the five States that have the largest population, to see if they can effectively deal with those populations.

Mr. HORN. Yes. Well, Los Angeles County, for example, when Mr. Condit and I held a hearing of Government Operations out there last year, we went over the figures, and some of them seemed a little soft to me, in terms of the county claims that they have about $1 billion in costs due to illegal aliens. There is no question that's true in the county hospital. There are tremendous—hundreds of millions of dollars expended in the emergency rooms dealing with the plight of illegal aliens, the births, so forth and so on.

But it would be, I think, helpful if GAO did an independent analysis, because otherwise you have the advocates and the detractors of doing something putting forth their numbers, and very frankly, all that does is lead to immobilization and confusion. If we could have something a little more solid, it would be helpful.

If there's a problem, let me know, and I will be glad to call Comptroller General Bowsher and see if we can't encourage this. I think Congress needs some independent voice here that isn't tied to the advocacy of this or that proposal or the detraction of this and that proposal.

Mr. REILLY. Perhaps, after the hearings, we can meet with your staff and get some specifics, exactly what kind of a study you would like, and we would be happy to pursue it.

Mr. HORN. Very good.

Are there any further questions from members of the committee? Representative Maloney.

Mrs. MALONEY. Following up on the chairman's points, at what point does protecting privacy become more important than identifying the last 1, 2, or 3 percent of the illegals?

Mr. REILLY. Well, the legislation that was proposed last year had severe penalties for people who violated privacy. And I think, in the final analysis, that's about the only way it will ever work, because whatever field of business you're in, whether it's in health or whatever it is, there are always going to be people who are going to violate privacy, whether it's for economic reasons or emotional reasons or whatever.

The only thing that I can think of that can stop them is if they have to pay a price. And I think that was the intent of the legislation that we saw last year.

You mentioned Mr. Condit, he was one of the people, I think, who was proposing that legislation.

Mr. HORN. That's right. And we held extensive hearings on that, and obviously one of the major areas of difficulty are the hospital and medical records of the country, where almost anybody can walk in and get access. There is not very good security. And I think a rather well-formulated piece of legislation did come out of the committee on this subject.

Mrs. MALONEY. Thank you.

Mr. HORN. All right. If there are no further questions, we thank you very much for coming over. Sorry you had to wait so long, but that's what happens with votes and interesting witnesses.

Mr. REILLY. It was an interesting afternoon. We learned a lot.

Mr. HORN. Good. That makes it all worthwhile then.

Now, can we have panel four come forward: Professor Eaton, Vice President Smith, and Special Agent Rasor. Mr. Meltzer, I apologize. If you would all stand and raise your right hands, we will swear you in.

[Witnesses sworn.]

Mr. HORN. All right. All the witnesses affirm.

Welcome. I have on my list first Professor Eaton, professor emeritus of the Graduate School of Public and International Affairs, University of Pittsburgh, on biometric identification technology.

Professor Eaton.

STATEMENT OF JOSEPH EATON, PROFESSOR EMERITUS, GRADUATE SCHOOL OF PUBLIC AND INTERNATIONAL AFFAIRS, UNIVERSITY OF PITTSBURGH; ROBERT RASOR, SPECIAL AGENT, U.S. SECRET SERVICE, DEPARTMENT OF THE TREASURY; AND RUSSELL MELTZER, DIRECTOR OF SECURITY, SCHLUMBERGER-MALCO, INC.

Mr. EATON. Representative Horn and committee, the hour is late, so I will not read my prepared statement.

Mr. HORN. As you know, if you were here, I said all of the prepared statements automatically go in the record in full, in lovely print, and we would like you to summarize in 5 minutes.

Mr. EATON. I prefer to make some comments on the thought-provoking discussion that went on here.

Mr. Velde summed up the issue that needs to be confronted. It has not been confronted by Congress for several decades. We have technology that allows us to reduce fraud to a very great extent.

Again and again, Congress has asked the various agencies, like the INS and the Social Security Administration, to propose what they would like to do, without being sufficiently aware of the political constraints of an agency that gets all of its funding from Congress and where they have offices in every State of the Union. They had better be careful not to antagonize too many of them. It's your enemies that make the problems; your friends often are not around to help you.

Mr. Velde pointed out that the truck driver system of identification and the advanced technology that is being used in some of the State drivers' licenses provide us with an optimum system for reducing fraud.

I'm addressing myself now not simply to the issue of immigration and employment verification. Between the President and the Republican-controlled Congress, you have the opportunity to cut the deficit of this country by a very significant amount without cutting any school lunch program or other worthwhile causes. What you can cut are the earnings of the criminal community.

I don't have an estimate, but 20 years ago there was a study which probably very few people even know about, a study of the cost of fraudulent crimes, and they estimated the cost of $25 billion. Whether it is $50 billion or $100 billion today, one would have to find out by careful study, but you can cut the deficit by reducing fraud, not only in producing documents.

A great deal of the fraudulent costs come from the fact that burglars are interested not in stealing minor personal items, they look for gold, for silver, for jewelry. If we had a way of inducing the

States to require that people who sell precious metals identify themselves with a biometrically generated ID card, there would be a lot of reduction of burglaries, because burglars don't go into our homes just for the fun of it.

We should also keep in mind that biometric indicators are a privacy-protective element. They do not reveal the person's sex, the age, the national origin. The fingerprint lines of a beauty queen are no different and no more interesting than the fingerprint lines of somebody who perhaps added too much weight.

So from the point of privacy, the only way we can really guarantee privacy and reduce computer hackers is to introduce the biometric measures, not only for aliens, but for people who have access to secret information systems. Now they only need a PIN system. In order to enter important data files, if they had to put their thumbprint on a reader and also enter their card, the digital components of their thumbprint, there would be a considerable reduction of this kind of fraud. In fact, it probably would stop it.

So, in conclusion, I would like to suggest that both privacy and security will be greatly enhanced if Congress has the courage to look at the technology that exists today and legislate so that the various agencies can do what they really would like to do, but feel it is politically unwise to even publicly propose. There are officials, Senators, and Members of Congress, who would object to such a proposal.

[The prepared statement of Mr. Eaton follows:]

Prepared Statement of Joseph Eaton, Professor Emeritus, Graduate School of Public and International Affairs, University of Pittsburgh

The nation owes a commendation to the members of U.S. Commission on Immigration Reform. Under leadership of Barbara Jordan, it has recommended an active search for "a simpler more fraud resistant (computerized) system for verifying work authorization". Similar recommendations were made by study commissions during the terms of Presidents Carter, Reagan and Bush. All of them became politically controvorsial and were under-funded. What this recommendation means in plain English is that if someone steals your wallet, he can use the dollar bills. But it would be risky for him to use your driver's license or the INS Green card. He might as well send them back to you and collect a finder's reward.

President Clinton and the Republican controlled Congress now have the opportunity to provide bi-partisan endorsement of this long overdue ID card reform. Fingerprints or other biometric indicators will have to be included if there is to be a significant enhancement in the efficiency of the identification and verification system. Valuable entitlements, such as the right to enter and to work in the United States, need to be verified by high quality identification documents.

My testimony will briefly summarize the pro's and con's of the available ID card technology. I also want to utilize how biometric indicators can be used to enhance our currently flawed data banks. Even the most confidential military or industrial data files are not now immune to being compromised by criminals and/or juvenile computer hackers.

Already nineteen years ago, the Federal Advisory Committee on False Identification alerted the country to the mega billion cost of crimes by persons masquerading under one or more false identities. Our nation attained world leadership in part by quickly incorporating technological innovations in our weapons systems. Civilian industries are also in keen competition to update their products by incorporating pertinent inventions. But when it comes to modernizing our grossly flawed personal identification methods, we have been much more cautious. This timidity exposes all of us, as individuals and as a nation, to helplessness in combating the widespread criminal use of false identification documents.

Biometric indicators are far less prone than Pin Numbers to being stolen or generated by invasive computer techniques. Loss estimates range from 25 to 100 billion dollars. Whatever the waste, it is real money, especially in the current budget deficit debate.

Biometric ID cards are increasingly used in moderate size business and government programs. Nearly every Federal employee, including all Presidents of the United States since Franklin D. Roosevelt, has been fingerprinted. The unique line pattern of each person's finger tips reveal nothing personal about them—not his or her sex, race, religion, national origin, sexual preference or marital status. Madonna's fingerprints are no more attractive than mine. This would not be true of our respective drivers licenses. Hers would be a collector's item, since it contains her photograph, her birthdate and her address.

Almost twenty years ago, the U.S. Immigration and Naturalization Service issued what were then called ADIT cards. Several versions included a machine readable digitally coded fingerprint. Congress did not balance the budget that year or since then, but it cut the modest funds needed to buy the machine readers that would have made it possible to verify these documents against the user's own finger-tip. This simple feature would probably have cut illegal immigration more than an extra 50,000 border guards, equipped with police cars and machine pistols.

No one is required to carry a drivers license, other than when they chauffeur a moter vehicle. Similarly, no one would need to carry their biometric ID card except when they want a Government entitlement or access a privacy sensitive or secret data file via their computer.

There is an added potential that could be derived from the Jordan Immigration Reform Commission proposal. If a biometric and machine readable ID Card were to be utilized, it could provide field tested evidence how large scale tamper resistant identity procedures could be adapted to reduce many crimes, especially tax frauds, drug smuggling, white collar and computer crimes on a nation wide basis.

The marketing of stolen goods by anonymous burglars through legitimate pawn shops and other businesses could be made much more risky if State Legislatures were willing to mandate more reliable identification procedures for persons trading in precious metals, diamonds and other valuable collectibles. Foreign terrorists, like those who tried to topple the World Trade Center and blow up Lincoln Tunnel in New York would find it much more risky in the future to enter, travel and leave the United States without detection.

This evidence notwithstanding, there continue to be members of the House and Senate who are concerned about the privacy threat from computerized data banks. Their immense capacity to store, analyze and retrieve is intimidating. They and their staff should consider setting aside a few hours between April 10 and 13th to visit the Washington Hilton Hotel. It will be hosting the annual Card Tech/Secure Tech conferecence, co-sponsored by the Biometric Authentification Consortium and the Federal Smart Card User Group. Well over 100 American and foreign corporations will be exhibiting their equipment and its technology. They can provide cost estimates of using their biometric card and machine readers system. They would also be able to discuss how data files could be protected against unauthorized access. Details can be obtained from Mr. Ben Miller, Conference Chairman at Phone 800–848–7242.

The utility of including a biometric indicator in important ID cards can be illustrated by the near ruination of Mr. Terry Dean Rogers. He came to the attention of the Saginaw, Michigan police, after they were called to investigate a noisy fight with his girlfriend. To his great shock, this part-time black college student found himself suddenly handcuffed, accused of committing two burglaries and two murders in Los Angeles, a city he had never visited. The prime suspect of the crimes, who had left his fingerprints at the scene, had used Mr. Rogers drivers license and other identity cards left in a wallet which had been stolen in Detroit, a year earlier. It was then marketed across the continent to a criminal who wanted a new identity.

What ultimately saved Mr. Rogers from a death row sentence was a FBI confirmation that his fingerprints did not match those of the criminal. But until that clearance made its way into the National Crime Information Center files fourteen months later, Mr. Rogers was arrested four more times in routine traffic checks. At each stop, the police radioed for an identity check. Each time Mr. Rogers was subjected to the indignity of an arrest with guns drawn by nervous policemen.

In conclusion, let me place into the record a summary of the evidence how biometric and machine readable ID cards can be used to enhance both our capacity to enforce laws and to protect our privacy. Both vital objectives can be advanced more effectively than if we continue to rely on our grossly outdated procedures. The United States should not enter the 21st century shackled to identification techniques that have made many of us victims of con games, burglars and the many other criminals who enjoy immunity behind a facade of false identity.

Only the criminal community enjoys a degree of privacy. People who pay their taxes share with anonymous clerks the most intimate details of how they earn and spend their money, child care payments for an illegitimate offspring or their gambling losses. In their physicians' offices, in hospitals and in the nationwide centralized data bank of health insurance companies, people with a venereal disease cannot hide their misfortune. Every one of us in this room has voluntarily shared more information with his video store, mortgage company and credit cards company than we can remember.

We all surrender a lot of privacy in return for the good life beyond the dreams of our forefathers—to travel without money and pay our bills with a credit card, to get a mortgage on our home from investors who have never met us and to rent movies to show in the privacy of our video. Hotels can keep records of who orders "x" rated pay films, data which few persons would want to have publicly disclosed.

No one running for public office is immune from character assassination. If there is anything even remotely embarrassing in their life history—let us say a ticket for speeding at the age of 16, with a beer bottle in the car, they have good reason to worry that the incident will be leaked in the next election campaign by an investigative reporter or an employee with access to the thirty year old pertinent record.

Milton R. Wessel and Jobn L. Lirley may exaggerate a little when they estimate that "that over half of our work force (is) busy producing, storing and transferring knowledge."[1] Much of it is secret and proprietary. Its privacy can be protected only by using the very same technology which allows us to keep it in digital data banks.

The following five techniques are available:

1. *Feedback to the Individual, Whenever a Privacy Sensitive Personal File Is Accessed*

Through reliance on biometric identity documents, all employees with access to our TRW credit rating, can be required to leave a trace of when and why they accessed our file. Their authorization to enter the data bank could be made subject to insertion of their ID card into a digital reader, verified at the same time by putting their thumb in another digital device. Only when the two machines record the same digital code will the computer permit them to access our file.

Few people would care to know when someone looks at their credit file. But should it matter to them, the data would be available at low cost. A single "print" command can generate a copy and another "mail" command can send the information to the person who requested it.

2. *Standards for Data Base Matching*

Comparison of different data sets is an increasingly important source of knowledge. Science lives on free exchange of information, including contradictions. The Internal Revenue Service could not function without the capacity to compare our claimed earnings to payments reported on W-2 and 1099 forms by those who had employed us.

For over 200 years in the United States the Census has succeeded remarkably well in preventing the information it is required to collect each decade from every U.S. resident from being shared with newspaper reporters, divorce lawyers—not even with the FBI and the CIA.

Paper files are hard to make secure. Anyone with access to an office door can sooner or later open a pertinent file drawer without being detected. Such an invasion of privacy becomes much more difficult in digitally stored data banks, where Data Base Matching must be preceded by an official authorization.

3. *Bonding and Licensing of Sensitive Data Bank Owners and Employees*

Not only physicians and attorneys need to be licensed. This requirement has been extended to many occupations—stock brokers, real estate sales persons, plumbers and electricians. The privilege of maintaining a privacy sensitive data file could be subjected to a similar requirement to maintain a reasonable level of security and an efficient procedure to expunge false or outdated information.

4. *Privacy Versus Freedom of Information*

The news media industry has succeeded having its rights to access information protected by the Constitution and a good deal of State and Federal Legislation. Privacy rights have a much more vaguely defined when privacy protection laws are

[1] Milton R. Wessel and John T. Kirkley, "For A National Information Committee", Datamation: 234–246.

passed, they will be more easily enforced when information is digitally stored in a computerized data bank than in handwritten or typed paper files.

5. Administrative and Legal Remedies

The almost infinite volume of information which is now being stored in computers would otherwise require vast amounts of paper and carbon copies. The world's supply of trees would be diminishing at an ever more alarming rate than at present. An occasional unintended and accidental leak cannot be avoided. Care wlll need to be taken to exempt these "accidents" from generating expensive litigation. They could quickly bankrupt even the most conscientious data bank operator.

A quite different standards should be applied to unauthorized data release for profit, for political purposes or to intentionally embarrass or harm an individual. The risk of such a lawsuit will also help to keep those who operate data banks them honest.

CONCLUSION

No person, except for criminals, can live in America without revealing a great deal about his or her private life. Privacy invasion begins at birth, when a baby's footprint is taken and, to issue a birth certificate, information is collected about its health and its parents. Before my children went to college, I was able to send for an extra copy of their birth certificate for two dollars each. A broker of false ID documents could have done the same thing. He could have enriched himself and the underworld with clone identities of my sons and daughter.

The enforcement of privacy rights requires that selected data files be subjected to digitally coded monitoring of persons who are entitled to enter information, analyze it, compare different files and then retrieve the outcome from a data file. This is now being done largely with PIN codes, which can be stolen or carelessly recorded in a person's wallet. Computer hackers have proven again and again that even the most secret PIN code can be broken.

Biometrically verifiable identity cards are much more secure. About the only way a computer hacker could gain access to the secret files of the CIA would be to invade its headquarters or one of its field stations, put a gun to the head of an approved operator and then force him to insert his ID document, while verifying it with his thumb, eye grounds, digitally readable handwriting or other operating biometric safety device.

The criminal hacker would be exposed to the risk that the hostaged CIA employee could activate a computer "red light" warning by inserting an "in trouble" code, such as pressing a digit in a normally forbidden manner.

No major invention or addition to knowledge can be reversed. Not even the most devout Mullah in Saudi Arabia who wants to imprison women who drive a car, can wipe out the evidence that the average woman driver has fewer accidents than males. What is technologically possible are computerized instructions to protect specified items of information from disclosure without a warrant from a judge or the permission of the person who generated the information.

Such a protective system would have to require that those who are authorized to access a confidential information data bank need to identify themselves with something more reliable than an access code or as a Pin number. Not even a social security card, a passport or a birth certificate, provides secure proof of identity. Nothing less than a biometric identifier which is transformed into a digital number pattern unique to each person, will provide us with reasonably secure privacy insurance.

Mr. HORN. Thank you. We appreciate your testimony.

The next witness is Robert Rasor, Special Agent, U.S. Secret Service, Department of the Treasury, on techniques for combating the forgery of Government documents.

Mr. RASOR. Thank you, Mr. Chairman.

As a law enforcement bureau of the Department of Treasury, the Secret Service historically has been charged with the suppression, detection, and prevention of violations of counterfeiting of U.S. currency and obligations. To that end, we also became the lead investigative agency relative to false identification, back in about 1982, pursuant to the passage of the False Identification Crime Control Act of that same year.

Counterfeiting or fraudulent identification initially does not seem as serious a crime as bank robbery, theft, or drug smuggling, until one realizes that fraudulent identification is really the basic necessity for all financial crimes, illegal border crossings, and fraudulent applications for benefits from local, State, and Federal Governments.

Fraudulent identification allows the criminal element to move freely through society, hidden from law enforcement and regulatory agencies whose duty it is to protect the nation's financial systems, borders, and benefit agencies. If our currency was counterfeited at the rate that false identification is being produced today, the impact would be dramatic to the economy and the confidence of the public in those same documents.

It is important to understand that in addition to just straight criminal investigations, the Secret Service has developed a proactive risk analysis process which, when coupled with existing enforcement expertise, has produced major successes in combating a broad spectrum of financial crimes by addressing system fixes in the banking, credit card, telecommunications, and government entitlement areas. The Service endeavors to prevent crimes by identifying the systemic weaknesses which allow recurring criminal activity. Once the weaknesses are identified, the Service attempts to address them by suggesting possible program management solutions.

For example, the techniques currently in place to corroborate identity are antiquated. Birth certificates, the initial documents needed to obtain a host of other documents, are easily obtained or counterfeited. Although counterfeit birth certificates and Social Security cards can and will be used to establish identity in the commission of financial crimes, it's the counterfeit driver's license that most often is used. That is due to the fact that drivers' licenses are easy to counterfeit, and during the course of business, the driver's license is the most popular and widely accepted credential in support of a financial transaction.

Because of these problems, we need to seriously review measures needed to improve these systems. We also need to make appropriate use of available technology to thwart this problem. The reliable and positive identification of a person's identity is clearly the most significant means to prevent fraud and related activities. Reliable identity verification systems are available in today's technological market. They have been useful for large government efforts to combat document-related crimes.

AFIS technology is currently being utilized in the automated fingerprint image reporting and match system in the Los Angeles County welfare program to verify the identity of all applicants and to defeat fraudulent application schemes. The AFIRM system was developed in response to multiple identity fraud cases in the Los Angeles general relief program and was later expanded for use in the aid for families with dependent children, the AFDC program.

AFIS can solve the problems associated with the unlawful use of counterfeit financial instruments and identification documents by linking personal identifiers with the use of the items themselves. AFIS technology in the Los Angeles County project is proving to be an effective tool in combating application fraud.

In closing, I would like to say the Secret Service supports initiatives which specifically incorporate measures designed to minimize fraud while still meeting program goals. These objectives are not mutually exclusive. To the contrary, incorporation of technology and systematic safeguards result in better resource allocations in both arenas.

That concludes my remarks, sir.

[The prepared statement of Mr. Rasor follows:]

PREPARED STATEMENT OF ROBERT RASOR, SPECIAL AGENT, U.S. SECRET SERVICE, DEPARTMENT OF THE TREASURY

Mr. Chairman, thank you for the opportunity to address this Committee on the subject of counterfeiting of documents and false Identification. I am Robert H. Rasor, representing the United States Secret Service in my capacity as the Special Agent in Charge of our Financial Crimes Division.

As a law enforcement bureau of the Department of the Treasury, the Secret Service historically has been charged as the lead agency in the detection, prevention, and suppression of counterfeit currency and Government obligations. To this end, the Secret Service became the lead investigative agency in false identification investigations as the result of the passage of the False Identification Crime Control Act of 1982. This legislation was intended to control the use of false identification in illegal immigration, drug trafficking, and flight from justice. In recent times, the use of false identification, as a vehicle to commit financial crimes, has become a priority concern to the Secret Service and the financial community. In 1994, the Secret Service investigated financial crimes cases totalling $1.5 billion. A majority of these cases involved false identification as a prerequisite to the crime. Counterfeit or fraudulent identification initially does not seem as serious a crime as bank robbery, thefts, or drug smuggling, until one realizes that fraudulent identification is the base necessity for most financial crimes, illegal border crossings, and fraudulent applications for benefits from local, State, and Federal Governments. Fraudulent identification allows the criminal element to move freely through society, hidden from law enforcement and regulatory agencies, whose duty it is to protect the Nation's financial systems, borders, and benefit agencies. If our currency was counterfeited at the rate that false identification is being produced, the impact would be dramatic to the economy and the confidence of the public in those same documents.

The United States Secret Service has had a number of opportunities this past year to testify before various congressional subcommittees regarding the problem of financial fraud and the myriad of attacks being directed at this Nation's economic system. The Secret Service is in a position to observe this problem as a result of its criminal investigative responsibilities concerning a wide variety of offenses, including financial institution fraud, credit card fraud, food stamp fraud, counterfeiting of U.S. currency, and the unlawful production and use of false identification documents.

In addition to conducting criminal investigations, the Secret Service has developed a proactive risk analysis process which, when coupled with existing enforcement expertise, has produced major successes in combatting a broad spectrum of financial crimes by addressing "system fixes" in the banking, credit card, telecommunications, and government entitlement areas. The service endeavors to prevent crimes by identifying these systemic weaknesses which allow recurring criminal activity. Once the weaknesses are identified, the service attempts to address them by suggesting possible program management solutions.

Secret Service investigations over the years have led agents to conclude there are two fundamental areas where commercial and governmental financial systems are vulnerable to attack: the introduction of fraudulent applications for entering into a program and the use of counterfeit instruments to successfully complete a wide variety of fraud within these systems.

Application fraud occurs when an individual applies for a loan, credit card, or even Government benefits in a fictitious name and produces false identification documents to assist in the scheme. This form of fraud allows the criminal to open, access and obtain funds from multiple accounts, thereby causing the Government and financial institutions to bear substantial monetary losses. Secret Service investigations have clearly identified a need for the implementation of better management and training programs to combat this type of fraud.

The second vulnerable area of financial systems relates to a criminal activity which uses "desk-top publishing" to counterfeit corporate checks, bonds, securities, and false identification documents. Criminal activities involving the production of counterfeit credit cards and false identification documents, counterfeit negotiable instruments, loan fraud and the use of fictitious bank accounts have increased dramatically over the past few years, due to the inexpensive and easily accessible computer and printing technology. Related to this increase is the emergence of organized criminal groups which are developing fraudulent schemes designed to simultaneously attack the various private and Government financial systems in the United States.

For example, techniques currently in place to corroborate identity are antiquated. Birth certificates, the initial documents needed to obtain a host of other documents, are easily obtained or counterfeited. Although counterfeit birth certificates and social security cards can and will be used to establish identity in the commission of financial crimes, it is the counterfeit drivers license that is most often used. That is due to the fact that drivers licenses are easy to counterfeit; and during the course of business, the drivers license is the most popular and widely accepted credential in support of a financial transaction.

Because of these problems, we need to seriously review measures needed to improve these systems. We also need to make appropriate use of available technology to thwart this problem. The reliable and positive identification of a person's identity is clearly the most significant means to prevent fraud and related activities. Reliable identity verification systems are available in today's technological markets. They have been useful for large Government efforts to combat document related crimes.

As an example, some law enforcement agencies utilize state of the technology in fingerprint identification through the Automated Fingerprint Identification System (AFIS). As described, this computer system serves as a depository of electronically scanned fingerprint files. This technology allows a quick comparison of these files when attempting to match fingerprint records. The Secret Service has experienced first hand the advantages and reliability of this technology. AFIS provides a means for the Secret Service to identify suspects in investigations and presidential threat cases by matching latent prints of unidentified individuals with a database of known records.

AFIS technology is currently being utilized in the Automated Fingerprint Image Reporting and Match (AFIRM) System in the Los Angeles County welfare program to verify the identity of all applicants and to defeat fraudulent application schemes. The AFIRM system was developed in response to multiple identity fraud cases in the Los Angeles general relief program and was later expanded for use in the Aid for Families With Dependent Children (AFDC) program.

A study of the AFIRM program was conducted by an independent audit firm who found the AFIRM system is accurate in that no false positive matches of applicants have yet occurred. The result of the audit indicate that the utilization of the AFIRM system has, to date, been successful.

AFIS can solve the problems associated with the unlawful use of counterfeit financial instruments and identification documents by linking personal identifiers with use of the bogus items themselves. AFIS technology in the Los Angeles County demonstration project is proving to be an effective tool in combatting application fraud.

In closing, the Secret Service supports initiatives which specifically incorporate measures designed to minimize fraud while still meeting program goals. These objectives are not mutually exclusive. To the contrary, incorporation of technology and systemic safeguards result in better resource allocation in both arenas.

Mr. HORN. Thank you very much, Agent Rasor. We now have Mr. Russell Meltzer of Schlumberger-Malco on how private consumer credit card charge authorization systems work.

May I first ask, is that firm related to the famous oil well technology company?

Mr. MELTZER. One and the same.

Mr. HORN. One and the same. When did they get in the consumer credit card business?

Mr. MELTZER. A whole month ago. They just became our parent company about a month ago.

Mr. HORN. I see.

Mr. MELTZER. Prior to that, they were heavily into the smart card arena.

Mr. HORN. And you were Malco before that, were you?

Mr. MELTZER. Correct.

Mr. HORN. Very good. Fascinating. I grew up running around their trucks as they pumped mud in various dry holes that my father was drilling.

Mr. MELTZER. Must be in the Long Beach area.

Mr. HORN. It was near there. It was Newhall and Monterey and other places that are now filled with houses, not oil wells, which shows the success of the family.

Mr. MELTZER. First of all, let me make a correction here. I just got the notification this morning about this meeting and was asked to appear here. My testimony is going to vary a little bit from what it is titled as, but I think it will draw the same conclusions.

I would just like to say, Mr. Chairman and members of the subcommittee, I would like to thank you for the invitation to appear before this committee. I wish to preface my testimony with the admonition that my time to prepare testimony was extremely limited, since I did not receive the invitation to appear before this committee until I arrived at my office this morning. So I feel somewhat amiss at what we really can present.

Mr. HORN. Well, we are grateful to you, may I say. The problem arose when the vice president of a major credit card company, who will go nameless to protect the guilty, was told by his general counsel he couldn't appear because he might reveal proprietary information, which is nonsense—so we are very grateful for you in sharing your experience at the last minute.

Mr. MELTZER. I know that individual, and I will be having a talk with him.

Prior testimony, government hearings, the news media, et cetera, have established the fact that the integrity of government documents has been comprised. Therefore, I feel there is no need to discuss or establish the facts of compromise. My testimony will address several issues which I feel are needed to institute a level of integrity to the documents.

It is well-known knowledge on the streets that documents can be duplicated, counterfeited, or altered; that when they are presented to employers, merchants, et cetera, there is no mechanism to authenticate these documents in a timely fashion. This appears to be a basis for a substantial amount of fraud that is perpetrated against the business community as well as the government.

The systems currently used by the government do not marry the document to the individual or authenticate the document itself. What I mean by this is that, when an individual presents an immigration document to an employer, there is no way for an employer to know if the document is counterfeit, duplicated, or altered. The employer has to base his decision on what he thinks his ability to discover a fraudulent document consists of.

With the quality of fraudulent documents today, the ability to detect fraud is definitely out of the range for the majority of employers. When an employer accepts the document, how does he know that the individual presenting the document is the true person the document was intended for, since the alteration of photos on documents seems to be second nature to the crooks today.

One has to remember that the era we live in today has been inundated with low-cost imaging technology and color printers, which has brought the ability to duplicate or counterfeit documents into the living room and out of the print shops or manufacturing arena. The expertise to utilize this equipment is at a high school level.

The technology to prevent the fraudulent reproductions or alterations of documents is no longer on the horizon but in existence today. Methods to protect systems that control documents have been in existence for a considerable length of time. The ability to marry a document to an individual is also in existence today. I will now offer some suggestions on how these technologies can be used to set up a system and issue documents that will maintain the integrity level we expect of a government document.

The theory of this system should be triangular in nature. Consider the three sides of a triangle as information, identification, and verification. This triangular system should be established along the lines of the credit card industry's authorization system. In essence, the government would be the bank, and the users of the system would be the merchants.

The government would maintain the data base which maintains the relevant information to identify an individual. The data base and the systems utilized to access it need to be projected through the use of an encryption process. Terminals like those used at point of sale in the retail community should be used to query the system. These would be considered public terminals that could be utilized by the business community, which, in this case, would be the government merchants.

These terminals should have the ability to query and not update or alter the information in the data base. When the ability to update exists, you now have presented the terminal with the ability to compromise the integrity of the information in the data base. The government, at their discretion, can place supervisory terminals that have the ability to update or alter information in the data base. These supervisory terminals would be required to have specific levels of security and access which now exist.

The second leg of the triangle is the document. This document should be of a smart card nature. This will give the document the required levels of security to prevent the counterfeiting or alterations of the document, as well as the ability to upgrade security at a later time. The smart card also presents the ability of marrying the document to the individual. This can be done with the use of biometrics.

The third leg of the triangle is the identification of the individual presenting the documents. This is accomplished through the use of a biometric system.

With the three legs of the triangle in place, you have the ability to authenticate the document, which is done by the data base; the ability to identify the presenter of the document, which is accomplished through the use of biometrics; and last but not least, you have the ability to tie the presenter to the document, which is accomplished through the biometric information contained in the smart card.

One has to remember that the weakest link in the security chain is the human element. If you want true security on a document, you have to remove the decisionmaking ability of the human element from the chain.

This concludes my testimony at this time, and I will be glad to answer any questions.

[The prepared statement of Mr. Meltzer follows:]

PREPARED STATEMENT OF RUSSELL MELTZER, DIRECTOR OF SECURITY, SCHLUMBERGER-MALCO, INC.

Mr. Chairman and members of the Subcommittee. I would like to thank you for the invitation to appear before this commttee. I wish to preface my testimony with the admonition that my time to prepare testimony was extremely limited since I did not receive the invitation to appear before this committee until I arrived at my office this morning.

Prior testimony, government hearings, the news media etc. has established the fact that the integrity of government documents has been compromised. Therefore I feel there is no need to discuss or establish the facts of compromise. My testimony will address several issues which I feel are needed to institute a level of integrity to the documents.

It is well known knowledge on the streets that documents can be duplicated, counterfeited or altered. That when they are presented to employers, merchants etc., there is no mechanism to authenticate these documents in a timely fashion. This appears to be a basis for a substantial amount of fraud that is perpetrated against the business community as well as the government.

The systems currently used by the government do not marry the document to the individual or authenticate the document itself. What I mean by this is that when an individual presents an immigration document to an employer there is no way for an employer to know if the document is counterfeit, duplicated or altered. The employer has to base his decision on what he thinks his ability is to discover a fraudulent document. With the quality of fraudulent documents today the ability to detect fraud is definitely out of range for the majority of employers. When an employer accepts the document how does he know that the individual presenting the document is the same person the document was intended for since the alteration of photos on documents seems to be of second nature for crooks today.

One has to remember that the era we live in today has been inundated with low cost printing technology and colored printers which has brought the ability to duplicate or counterfeit documents into the living room and out of the print shops or manufacturing arenas. The expertise to utilize this equipment is at a high school level.

The technology to prevent the fraudulent reproductions or alterations of documents is no longer on the horizon but is in existence today. Methods to protect systems that control documents have been in existence for a considerable length of time. The ability to marry a document to an individual is also in existence today.

I will now offer suggestions on how these technologies can be used to set up a system and issue documents that will maintain the integrity level we expect of a government document. The theory of this system should be triangular in nature. Consider the three sides of the triangle as: information, identification and verification.

This triangular system should be established along the lines of the credit card industry's authorization system. In essence the government would be the bank and the users of the system would be the merchants. The government would maintain the data base which maintains the relevent information to identify an individual. The data base and the systems utilized to access it need to be protected through the use of an encryption process. Terminals like those utilized as point-of-sale in the retail community should be used to query the system. These would be considered public terminals that could be utilized by the business community which in this case would be the goverment merchants. These terminals should only have the ability to query and not update or alter the information in the data base. When this ability exists you have now presented the terminal with the ability to compromise the integrity of the information in the data base. The government at their discretion can place supervisory terminals that have the ability to update or alter the information in the data base. These supervisory terminals would require specific levels of security and access.

The second leg of this triangle is the document. This document should be of a smart card nature. This will give the document the required levels of security to prevent the counterfeiting or alteration of the document as well as the ability to upgrade security at a later time. The smart card also presents the ability of marrying the document to the individual. This can be done with the use of biometrics.

The third leg of the triangle is the identification of the individual presenting the document. This is accomplished through the use of a biometric system.

With the three legs of the triangle in place you have the ability to authenticate the document which is done by the data base. The ability to identify the presenter of the document which is accomplished through the use of biometrics. And last but not least you have the ability to tie the presenter to the document which is accomplished through the biometric information contained in the smart card.

This concludes my testimony. I know I have presented my position here today in a brief simplified manner. If the technologies I have elaborated on are put into use by the government I strongly feel there will be a great impact on the fraud picture as we see it today.

Mr. HORN. Thank you very much.

Representative Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman.

A number of witnesses have testified earlier today about how easy it is to forge a birth certificate. From a birth certificate, one can then get a passport, a license, and probably a green card. How would we first deal with securing the birth certificate?

Mr. MELTZER. Is that for any of us?

Mrs. MALONEY. Any of you.

Mr. MELTZER. First of all, you would have to go to a different technology. Birth certificates, as they exist today, I don't think can be prevented from being compromised. They are a paper document. Most people transport this document, even with the certified seal that most counties put on, to a place that accepts it. So all they are accepting is a piece of paper with some notations on it and some type of stamp.

Again, with the imaging processes out there today, you can duplicate anything. One has to keep in mind the theory behind these imaging processes is to make a duplication of something without your being able to notice that it has been duplicated. So I think you would have to go into some new technology, if you really want to start at the basis, and again, maybe you have to issue a smart card at this time, with certain information in there that can't be altered. If you try to crack that chip, it all just turns to mush on you.

Mrs. MALONEY. We routinely read stories about counterfeit smart cards, credit cards. What is the extent of this problem?

Mr. MELTZER. Not counterfeit smart cards; counterfeit credit cards, yes. The majority of cards that are counterfeited are all mag stripe type cards. That's why the card-issuing industry is moving to the second level of technology or the second generation of cards, which will be the smart card.

In Europe, you will find that the majority of cards that are being compromised over there that are——

Mrs. MALONEY. Is that a biometric card? What's a smart card?

Mr. MELTZER. A smart card is a chip card.

Mrs. MALONEY. A chip card.

Mr. MELTZER. Right. The terminology is one and the same. It's an integrated circuit chip placed in your credit card, and that's like a little computer chip that contains all the information you put in. You can put in different levels of security in there, depending on how elaborate you want to get. These systems can be tailored to your specific needs that nobody else has access, or they can be tailored to where there is a public key access.

In Europe now, France has gone totally to the smart card. There you are seeing a lot of fraud, but when one analyzes that fraud, they currently have dual——

Mrs. MALONEY. Fraud with the smart card?

Mr. MELTZER. Yes. They have dual technology on that card because they are unable to use the card outside of that country. So, therefore, they have a mag stripe on it, so it's still a universal payment tool that can be used in any country. When they take it and utilize the stripe, again, the stripe can be compromised.

We're seeing a lot of counterfeiting of the mag stripe, alterations of the stripe, skimming of the stripe. That stripe is strictly a magnetic piece of recording tape that has information on it. So where they have a total use of the smart card, you do not see any compromise of that smart card, to my knowledge, to date.

When the smart card comes in here, you're going to probably see some fraud for several years, because when the smart card comes into the United States, you're going to have dual technology: you will have a chip in the card, and you will have a stripe. Because as they put the readers in, they are not going to just flip a switch and there will be smart card readers from coast to coast. You are going to have them migrate through the areas, and they will probably start in the high fraud areas first, would be the rational business plan.

As long as you have that stripe, all you have to do is disable that chip. If you go into a merchant who has a smart card reader, he is going to fall back on the backup technology or the secondary technology which will be that stripe, for several years to come. Once the chip is totally implemented, I can't say there will be no compromise of that chip, but the compromise that could exist compared to what we have today would be a drop in the bucket.

Mr. EATON. Let me give a simpler suggestion.

Mrs. MALONEY. Could I just follow up? What does that tell us about creating a secure national ID system?

Mr. MELTZER. From my law enforcement background and being in the banking world for a while, prior to being in the manufacturing world, every time I hear that I have to chuckle to myself, because if you really look at what we have in this country today, tell me we really don't have a national ID system.

If you want to work, you have to have a Social Security card. If you want to claim your newborn as a dependent, you have to have a Social Security card. If you're an immigrant coming into this country, you have to have an INS card. Between those two data bases, I don't know who is not covered.

Now, it's just a matter of terminology. I think it just depends, are we willing to admit it or not? I know civil libertarians scream when you mention this. But, you know, to me, I live in a real world. It exists. Look at a driver's license. Anybody of the age of, what, 17 or 18 now, who can legally drive, I hardly know anybody who doesn't have a driver's license.

But if you start looking now from birth to death, in this country you're going to find a Social Security card. Is that a national ID card? I don't know. Is it voluntary? To a degree.

Mrs. MALONEY. And you wanted to add, sir?

Mr. EATON. Yes. To do anything about the 262 million people who are now living in the United States would be very expensive.

But every new baby born, at least in most hospitals, gets footprinted in order to prevent mixing up of babies. The technology exists to digitalize these indicators and thereby issue the kind of card that Mr. Meltzer is suggesting, with a digitalized identifier that relates to each particular baby. At a later time, the birth certificate can be updated to a simpler biometric indicator, where you don't have to take your shoes off, and thereby gradually improve the identification system.

What we need to do—and this is, again, something that Congress has to address; namely, the fact that birth and death certificates are being issued by over 4,000 different jurisdictions. We need to find some way of inducing all of these jurisdictions, by some kind of a carrot program, to accept uniform standards. In 25 years we will begin to make it more and more difficult for persons to forge birth certificates.

Until we can do that, we have to go with the fact that the kind of improvements that have been suggested will probably reduce the amount of fraud by maybe 75, 80 percent, not absolutely.

Mrs. MALONEY. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. Thank you, Representative Maloney.

Let me go down the line on a few questions here. You have heard Mr. Velde's comments on the various motor vehicle linkages across the country, where generally they do see the person, take the photo, get the fingerprint, et cetera. So one option here is the existing 50-State system of either State identification, State motor vehicle licenses, and so forth, and to link that with some of the other ones that are already being linked, in the sense—the Brady bill was mentioned and others.

What is the reaction of this panel to that? Or should we try to go for this great massive national approach, which people have talked about for years but never seems to be getting anywhere. There are constant demonstration projects but nothing much happening. What's the feeling of you experts, in terms of the evolution of what is already there and networking it together versus sitting around hoping something will happen?

Mr. EATON. Well, I would go for the State driver's license system for two reasons: The States are closer to the individuals than the Federal Government. If the Federal Government sets up, through legislation, standards for drivers' licenses, in return for which States are eligible for certain programs—even without that carrot, probably more and more States will accept the same or comparable technology. On that basis, I believe we can greatly reduce the fraudulent use of identity documents.

Mr. HORN. Mr. Rasor, do you have any feelings on that?

Mr. RASOR. Well, I would tend to agree with the professor's comments relative to the importance of drivers' licenses. I would say that there probably is no single solution to the problem.

I think that you have to understand that what we have moved from is a system that used to rely on a document as being genuine and representative of either a right or a privilege or an identification, and basically due to today's desktop publishing problems, there basically is no such thing anymore as something that cannot be counterfeited, that cannot be replicated to be exact in every dimension as the original.

So whatever you do, you have to tie the identification symbol to the individual. And there are, as I said before, a number of ways that that can be done. But what you're going to have to end up with is the ability for society at large to be able to rely on the fact, when somebody needs to present an identification document for a particular reason, that it's a reliable system. The system right now doesn't do that.

It's tying, by a biometric identifier, a person with a card. It would be for others to say what the expenses of that are, what the practicalities of that are. Our job here is to point out the fact that there are multiple attacks on the system as it currently stands and that a change does need to occur.

Mr. HORN. Mr. Meltzer, do you have any feelings on that?

Mr. MELTZER. I think the States are going in the right direction; it's a step forward. But, again, I think it's time that the government has to make a decision: At what level are we going to accept accomplishment, if we solve 60 percent of the problem, 70 percent of the problem, or do you want to shoot for 100 percent of the problem?

Again, I'm not in a position—I'm not affiliated with the government, so I really don't know what the views of the government are. But from a private standpoint, I think that there are ways to go 100 percent on the solution. I see there are ways, I feel, to probably utilize a single card without calling it a national identity card, to give a lot of the benefits to people that they have coming from the government.

If you stop and think, you're coming out with an electronic benefits card. OK. If you move to the smart card arena in that, within a chip in the card, you can add all kinds of stuff, all your Social Security, the same card can have immigration stuff in. Anything else in that the government wants the holder to have you can put in one card, with one chip.

Of course, if you lose that card, you have to go back and get a new one, and it has to be reloaded with everything. Then you would have to take a hard look at the design of your data bases because they would have to talk to each other, so when you download to this chip, you know what you are downloading.

One of the biggest problems banks find, as they are growing, their data bases are fragmented. You've got a million computers. You've got a million computer horsepower there, but none of them talk to each other. So every time you have to try something to move information across the spectrum, it's almost impossible, or you have to design a third or fourth data base to do it.

So it just depends which way the government wants to go. I think the technology is there. I know you have a very big problem when it comes to privacy, but if you approach these systems correctly, with the right technology, privacy is built in.

You go into the encryption of this information; you say hackers are running all over. You will find that most systems that hackers get into are not encryption-protected. You will find stuff that's intercepted on wires is being transmitted in the open, not in encryption mode. So there is stuff there. If you want to get into that, you've got a powerhouse of information not too far down the street in NSA, as far as encryption goes. To me, those guys are the brainpower in that field. You have a lot of cryptologists there. There is information you can seek there.

If you want to take a look at the rest of the problem, then you're just going to have to figure out, what do you want to put and where do you want to put it? I still think one card would be nice, and I think it would be a savings to the government if you had all your benefits on one card. And the one that you give out for immigration, all you have to do is hand this card to the employer. You have the ability now, you can plug the card into a point of sale terminal, and it comes back and says go or no go.

That same card can be used to secure the information, because you can set it up where you cannot get into that computer unless you plug your card in. That's going to tell you who is on that computer, what period of time. And if you want to set it up, there are all kinds of audit procedures on a computer. You can tell exactly what key strokes the guy made. So security is there. It's just, do you want to implement it?

Mr. HORN. One of the problems you face when you're trying to check for illegal, undocumented aliens is, if families are hiring one or two people, if small businesses are hiring one or two people, the expense of getting one of those machines to check the card is a little much. So you're going to have to resort either to an 800 number or something like that, where there is a convenient way to check the card.

Is that possible with what you're talking about, that somebody on the other end can punch the right numbers and check it?

Mr. MELTZER. One of my favorite sayings is: Remember, security is not a convenience; it's an inconvenience. The more security you have, the more inconvenience you have. This could be set up probably where there could be a Social Security office, various governmental agencies around the city. When you finally make your selection on this individual is the time you're going to want to authenticate this, not when you're going through the approval process or selection process. And it may have to come to the point where you're going to have to say, "I'm going to hire you. Let's go down to this office, plug your card in, and this will say yea or nay, if you qualify."

Again, it's an inconvenience, but sometimes, if you want certain results, you have to put up with inconveniences. We work strictly in a secure environment in our plant. We manufacture credit cards, you know. When you have a $100 bill stolen from you, how much have you lost? $100, not a penny more. You can't get penny more on the street. But credit cards, in essence, they are printing plates for money, so we really worry about it.

We have to do backgrounds on all of our employees, and we find a real problem in trying to get information, because we don't know who we're hiring. We run fingerprints, but, again, it takes 8, 10, 12 weeks for those to come back. Meanwhile, you put the guy in the cash vault. If he's not who he says he is or his intents are wrong, we're out of business. So these are problems.

When immigration regulations come into play, we take a look at the individual. He handed me a document. I was in law enforcement for 23 years. I look at a document, can I tell if it's counterfeit or not? I used to be able to, no longer, not with the quality out there.

So how does John Doe, average employer, get over this? You know what, ignorance is no defense of the law? So he's in trouble if he makes the wrong call.

Mr. HORN. Mr. Rasor, do you have any help or advice you can give us on that?

Mr. RASOR. Well, I mean, I come back to, you know, this problem, as I've mentioned, transcends a number of the issues here today. It goes to the essence of a government expending funds for one function or another and having the ability to be assured that where that money is going is proper and complete.

I would put one more thought into the record and that is, the Secret Service spends a great deal of time talking to the financial industries: the banking community, the credit card community, the ATM systems around the country. One thing that we insist upon is that their systems become as complete as possible, because the violations that occur, that are a violation of Federal law, are time-consuming and draw down on resources of law enforcement, generally, to investigate those crimes.

Where those crimes have systemic or technological fixes and they become repetitive and cyclic, nobody wins. So I would say, in our process here, we should look to the various safeguards that we really demand of the private sector and make sure that we at least match that, probably learn from that, and try to get ahead of where that situation currently exists. Even with all the efforts they put in, they have tremendous fraud losses. So I think that needs to be blended.

Mr. HORN. Dr. Eaton.

Mr. EATON. Well, the employer of a small number of persons, for him, every hiring is important for his business. In our homes we want somebody checked who looks after our children as much as possible. We spend hours interviewing and calling references.

So the idea my colleague here suggests, that you go down to one of the Federal offices and check the card, is really not a great burden. Quite the contrary, I think it would be a great relief to both employers and people who hire household help to be able to verify the qualifications of the people they hire much more than they now can.

Mr. HORN. I was just thinking, if you take them to the office, one door would be, you passed, and the other is, you're boarding a plane to go back to the country from which you illegally entered. Representative Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman.

How would biometrics work or help with ordering by phone or from a mail catalog?

Mr. EATON. Well, biometrics, after all, the fingerprint doesn't get transmitted; it's the digital equivalent of the fingerprint which can be read electronically. So the capacity to use it is very much the same as the capacity that we use our credit cards now, when we push them through a reader.

There are some problems. I mean, there is no 100 percent solution, even with biometrics, because of the possibility that people who have high technology can take the biometric indicators from the transmission system. But there would be tremendous reduction of fraud.

And I would like to add one more thing, why I think it is unfortunate that Congress has so far not really been responsible in looking at this technological problem that deals with the issue of national security.

We are living in a period where fanatics are targeting this country—and the World Trade Center was just one example. There are technologies out there that are far more dangerous than explosives; namely, biological warfare. For its use you don't have to have a high degree of technological sophistication. If you have the material to spread disease, you can go to a paint shop and get one of these dispensers that sprays paint, and go and drive 10 miles from a military base and create havoc.

So the capacity to use ways and means not only to control ourselves internally, but gradually, because of the cooperation among most nations with passports, we have the capacity to make it extremely difficult for professional terrorists to travel around the world as freely as they now do. They may be able to do it once, but once they are identified, if airplanes just are able to get the digital readings of the fingerprints of their passengers, we have a control mechanism that will greatly increase the capacity of the Secret Service to be effective.

Mrs. MALONEY. Thank you very much.

Mr. HORN. Thank you.

Let me ask a few questions here. Some we will submit in writing, but let's round this out. Let me go back to the basics. You've mentioned it. What is the data encryption standard, or DES? Is it in common use today? Is it becoming obsolete, or is it already obsolete? What's the fast reaction to that one?

Mr. Meltzer.

Mr. MELTZER. Well, I know DES is in effect today. It's in effect in many things. As far as it becoming obsolete, I'm not a cryptologist. I don't think I can answer that. I think that's an answer that, one phone call to NSA and they can tell you about it.

Mr. HORN. How about it, Mr. Rasor?

Mr. RASOR. That's over my head, sir.

Mr. HORN. Mr. Eaton.

Mr. EATON. Same here.

Mr. HORN. All right. If we get into the groove of relying on the cutting edge of technology to guard against fraud in government documents, is it likely we will have to reissue the tamper-resistant documents in ever more sophisticated burgeons every few years?

Mr. MELTZER. If you pick the right technology, it's upgradable, as I mentioned about the smart card.

Mr. HORN. And you think that's the basic technology that needs to be picked.

Mr. EATON. Well, I'd like to say something else. We are now using a technology that is, in many areas, over 100 years old.

Mr. HORN. You mean fingerprint or——

Mr. EATON. With what is going on now, there will be improvements, but I think much of it is upgradable. And the fact that we are still using this very primitive technology—when my children went to college, I decided they needed a birth certificate. So I called Detroit, where two of them were born, they said, "Send us $2, the name of the hospital where they were born, and their birth dates." I got their birth certificates. You could have gotten their birth certificates, too. And that's still the way you can do it.

So if we just go from a 100-year-old system to the present technology. we will be much better off.

Mr. HORN. Well, that leads me to my next question to Mr. Rasor. Given the Secret Service's jurisdiction over the production and transfer of non-Federal Government identification documents, such as birth certificates and drivers' licenses, what power or authority does this convey over State vital records or motor vehicle administration offices? Is the Secret Service working with the States and localities to develop a standard document and security formats?

Mr. RASOR. Well, the question is twofold. What power does it give us?

Mr. HORN. Right.

Mr. RASOR. It gives us no power. In a partnership type arrangement, based upon the whole process of the risk analysis assessment that we do with the criminal investigative work, we do go to the States. We have an agent assigned basically in every State to be the false identification coordinator.

The first step in that process was just to collect the valid existing identifiers that the State produced. In other words, a State may have 8, 9, or 10 different drivers' licenses. You know, we believe that that system can be improved, and we try, within the limits of what we have available to us, to encourage changes to make the systems more verifiable and more complete.

Somewhere along the line, if one of these systems becomes complete, it can stand as the base for all other systems. It's either in the driver's license or the Social Security card or someplace else in a system where you might get a completeness and be able to rely on that.

That's a long answer to your question. We're trying, sir.

Mr. HORN. Yes. Well, I think that's very commendable, because, as you say, my heavens, it's a wonder the States have any coordination of this. Are there State laws primarily on the books now where there is a common birth certificate in some of these States? Are there any interstate compacts that relate to birth certificates?

Mr. RASOR. I don't know the answer to that question, specifically. I can find that out for you and report back to you.

Mr. HORN. I would appreciate it, and we will put it at this point in the record.

[The information referred to follows:]

The Secret Service has an agent in each state designated as the "ID" coordinator. This agent maintains a liaison with the state agencies that issue identification documents. This allows the Secret Service to collect and maintain genuine samples of identification documents to use for comparison purposes in analyzing counterfeit identification documents. It also gives the Secret Service the opportunity to offer advice on methods that would make current identifications more difficult to counterfeit. For instance, our "ID" coordinator in Albuquerque, New Mexico, has been providing assistance in the re-design of the New Mexico driver's license.

Re-designing existing systems only provides a temporary fix to the significant problem of counterfeit identification. Technology, primarily through the use of computers, has made current systems of identification obsolete. The Secret Service has determined that the only reliable method of identification of an individual is through the use of personal identifiers. Reliable identification is available in today's technological markets through the use of the Automated Fingerprint Identification System (AFIS). AFIS technology, through the use of inkless scanners, allows for a positive verification of an individuals identity. AFIS technology could be adapted for all forms of identification documents, including driver's licenses and birth certificates.

The Association for Vital Records and Health Statistics (AVRHS) is concerned with the increasing fraudulent use of vital records. The AVRHS has approached the Secret Service about the feasibility of convening an ad hoc group state and federal agencies to examine what should be done to combat the problem of false identification. The Secret Service plans to set up a meeting to discuss the counterfeiting of vital records documents. This could be an excellent forum to discuss-new formats of vital record documents which allow the states to maintain their individual identity, but at the same time place common features in these documents so they are more easily recognized.

Mr. HORN. You mentioned two fingerprinting systems. The acronym AFIS is one, and AFIRM is the other. They appear to be effective and accurate. Can you comment on the new, supposedly more advanced system being developed by the FBI that allegedly won't be able to talk to either AFIS or AFIRM, and aren't these two existing systems unable to do Brady background checks for gun purchases?

Mr. RASOR. Sir, I'm not familiar with that. The best answer to that would come from the FBI.

Mr. HORN. OK. Staff will ask them.

Is the Secret Service assisting State, local, and Federal agencies to link their data bases in pursuit of counterfeit and false identification problems, and is a network of State drivers' licenses with INS and SSA data bases, for employment purposes, feasible in your estimation?

Mr. RASOR. On the first question, yes, the Secret Service works closely with the State agencies in encouraging the linking and actual use of the linking of the AFIS systems throughout the United States. We have found that a very beneficial process in our investigative responsibilities.

In relation to the other question relative to the INS data base and the Social Security data base—is that what you were talking about?

Mr. HORN. Yes. Right.

Mr. RASOR. Being on the outside of that issue, I don't know the practicalities of it. I can tell you, in theory, that we would support the theory of the data bases within the Federal Government being able to talk to one another for two reasons, really: the responsibility that the program agencies would have in maintaining their system and protecting the fraudulent attacks on those systems as we see them occurring.

Mr. HORN. Is there a coordinating agency within the government, let's say in OMB somewhere, that looks at these data bases when they are proposed by departments and sees if there is some interchangeability and compatibility and all the rest, or how does that work? You just pick the best system you think helps your needs, and off you go, if you can get it through GSA and Congress?

Mr. RASOR. Again, I wouldn't be your best witness on that. I really don't know the answer to that.

Mr. HORN. Let's ask staff to check on that one also.

Dr. Eaton, you're familiar with a lot of national identification systems in European countries. How do these systems work, and do they affect privacy more so than the present systems affect American privacy?

Mr. EATON. Well, in many European countries, the government has appointed a privacy ombudsman to which an individual can come and complain if his or her privacy is violated, without a lot of expense or complication. These people are underemployed. There really aren't that many violations, especially if the violations become a source of punishment.

Let's even think now in the United States where we have a tremendous amount of information that all of us voluntarily provide. The only people who have any real privacy are the criminals. You and I, who pay our taxes, we don't have any privacy. When you go to a hospital, you don't have any privacy, and there is a central data bank that gets ahold of all the information of what they medically did to you, so that if you want to apply for insurance and don't tell them what your problems were, they catch you.

We don't have much privacy. But I believe the best protection about privacy, and that is not being used now in Europe, is to require a licensing of agencies that hold sensitive personal or security records. And part of the licensing is that they have a procedure, which several of the panel members have already referred to, where the people who access a data base have to leave a record of who they are, a biometric record, of the time and the length of access.

So if at any time you become suspicious that, let's say, some lawyer got ahold of private information about you, you are able to check. This is not now possible. This is also not now possible in most countries of Europe. But the possibility is certainly there, technologically. In some private corporations, they already have mechanisms to make sure that, when you enter one of their data banks, it is recorded who you were, how long you were active, and what you did.

Mr. HORN. Very good. If there are no further questions on the part of the ranking minority member, I see none on the part of the majority.

Let me just say, thank you one and all. We appreciate your staying a little late. I apologize to all the significant others involved.

And I want to thank the staff director, Russell George, and his staff, particularly Tony Polzak who is to my left, the counsel on this investigation, who is a legislative fellow with the committee, and Wallace Hsueh and Andrew Richardson of the staff. Thank you very much, gentlemen, for putting the hearing together. We appreciate it.

The hearing is adjourned.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF LAMAR SMITH, VICE PRESIDENT FOR GOVERNMENT RELATIONS, VISA U.S.A

Mr. Chairman, I am pleased to respond to your request that I appear today before the Subcommittee on Government Management, Information and Technology. My name is Lamar Smith. I am Vice President for Government Relations at VISA U.S.A, a part of VISA International.

VISA credit cards are issued by more than 21,000 financial institutions around the world. The company that I work for, among other things, maintains the worldwide telecommunications and data processing network that makes possible use of those VISA cards at more than 12 million merchant locations worldwide. One function of that network is to authorize a merchant to accept a VISA card when a customer presents the card as payment. In this way, the telecommunications and data processing network is a key element in protecting the integrity of VISA cards.

Various features encoded on the credit cards themselves also are used to protect the integrity of the cards. VISA works with the 21,000-plus financial institutions issuing VISA cards to help develop the security features that will enable these issuing institutions protect the security of their cards.

Having discussed with Subcommittee staff how I might be helpful to you, I will briefly discuss the general nature of these two categories of security protection: (1) the security features on cards themselves and (2) the authorization network. As I told your staff, I cannot discuss some of the details of these systems in a public forum. Attached to my statement are: (1) a reproduction of a typical VISA credit card, and (2) a diagram of the authorization system used to authorize a merchant to accept a VISA card presented as payment. A diagram of the settlement system used to make payment from the cardholder's bank to the merchant's bank also is attached to outline another function of the VISA telecommunications and data processing network.

SECURITY MEASURES ON THE CARD ITSELF

Looking at the reproduction of a typical VISA credit card, the security measures on the card include the following:

1. There is a four digit number printed just above the embossed account number that must match the first four embossed numbers on the card.
2. The characters and letters embossed on the card are clear and uniform in size and spacing.
3. There is a special "Flying V" embossed security character that appears with either the letter "C," "P," or "B" on the same line with the valid dates.
4. There is micro printing around the VISA logo. It is made up of the first four digits of the account number and an alpha designation.
5. A dove hologram appears to fly when tilted back and forth.
6. While not shown on the reproduction of a card, the Signature Panel on the reverse side bears the repeated word "VISA" in blue at a 45-degree angle, and this will fade if erasure is attempted.
7. Also not shown on the reproduction is an ultraviolet dove on the face of the card visible by use of a "black light."
8. Finally, some VISA issuers are putting digitized photos of cardholders on their cards.

SECURITY PROVIDED BY THE AUTHORIZATION SYSTEM

Turning to the authorization system, in the bankcard industry, banks that issue credit cards to their customers are known as "issuers." Banks that collect funds on behalf of merchants for sales made on credit cards are known as "acquirers." Following the steps in the authorization system:

1. A bank issues a card to the cardholder;
2. The cardholder presents the card to a merchant as payment for a good or service;
3. After the merchant "swipes" the card through a point-of-sale terminal that automatically reads information on the card's magnetic stripe and the merchant enters the amount of the proposed purchase using the terminal's keypad, the terminal automatically transmits an encrypted authorization request to the merchant's acquirer;
4. The acquirer routes the encrypted electronic authorization request to Visa over the BASE I network;
5. Visa automatically routes the request to the card issuing bank;
6. Upon receiving the message, the issuer electronically checks the cardholder's account;
7. If the card has not been reported lost or stolen and the account is in good standing with the cardholder having sufficient unused credit in his or her line to cover the charge, the issuer sends an "authorization code" number back to Visa over the BASE I network;
8. Visa adds a "transaction code" number to the authorization message and routes it back to the merchant's acquirer; and
9. The acquirer sends the authorization code to the merchant's point of sale terminal.

When this electronic authorization system is used, Visa's objective is to take no longer than 2.3 seconds to process the authorization request and complete delivery of the authorization code back to the merchant.

CONCLUSION

Two general categories of security measures are used to protect the integrity of VISA cards: features on the cards themselves and a telecommunications and data processing network for virtually immediate card authorization. New technologies such as chip cards are under development to further enhance security. In evaluating past and future technologies, of course, the cost of a technology and the acceptable time frame for determining the integrity of the card are critical considerations.

I am here to try to answer any further questions you may have.

[Whereupon, at 6:15 p.m., the subcommittee was adjourned.]

○