TESTIMONY OF ASA HUTCHINSON
UNDER SECRETARY
DEPARTMENT OF HOMELAND SECURITY
DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY
BEFORE THE SENATE COMMITTEE ON FINANCE
SEPTEMBER 9, 2003

Chairman Grassley, Ranking Member Baucus, and other distinguished members, I am pleased to be here today to testify about homeland security and the potential threat of terrorism presented by document fraud, identity theft, and the misuse of Social Security Numbers**.**

As you know from Congressional hearings, GAO investigations, and press reports, it is certainly possible today to produce or acquire false documents and gain entry into the United States. The Department of Homeland Security and the Directorate of Border and Transportation Security are working actively to address this problem in a number of ways, as I will detail in my testimony.

Despite all these good efforts, we, and the Congress, must be realistic about the results to expect. While we can, over time, reduce the instances when false or fraudulent documents are used to enter the U.S. or to obtain some governmental benefit, there is no easy fix available, and this is a long-term issue for the Congress, the Administration, and DHS to work through together.

DHS is working diligently on all these issues, and my staff has had several meetings with the Social Security Administration to discuss issues of mutual concern and potential ways to reduce the instances where Social Security Numbers are misused.

Description of the Problem

Document Fraud

Fraudulent documents, and, equally as important for the purposes of this hearing and our enforcement efforts, legitimate documents issued as a result of the use of fraudulent "breeder" documents can and are likely used to gain entry into the U.S. and to obtain federal and state governmental benefits each and every day.

As a general rule, the Immigration and Nationality Act requires all U.S. citizens to present a valid U.S. passport to enter or leave the U.S. There are several exceptions to this general rule. The most important applies to travel to and from the U.S. involving "any country, territory, or island adjacent [to the U.S.] in North, South, or Central America excluding Cuba." Thus, as a matter of law, U.S. citizens do not typically need to present a single document -- a passport -- to reenter the U.S. for any travel in the Western Hemisphere.

As a U.S. citizen is not required to present a passport for reentry, federal regulations do not detail what is necessary to validate a person's claim to citizenship in a manner equivalent to that of a passport.

The law requires that a person claiming to be a U.S. citizen "must establish that fact to the examining officer's satisfaction." [8 C.F.R. 235.1(b).]

In operational practice, our inspectors from the Bureau of Customs and Border Protection (CBP) examine any document that may establish identity and place of birth, such as a U.S. birth certificate, driver's license, or whatever else the person's basis for claiming citizenship might be, including baptismal certificates, Certificate of Naturalization, Report of Birth Abroad of U.S. Citizen, or Certificate of Citizenship.

No law or regulation prevents an oral claim of U.S. citizenship in these circumstances. An inspector may, and often does, ask for documentation to support a claim, but this is not currently required. Thus, even if an individual lacks any documentary identification or, as in the case of the GAO investigators who will testify later, the person presents counterfeit documents, inspectors must let the individual back into the U.S. if the inspector is satisfied that the individual really is a U.S. citizen.

By law and practice, CBP inspectors cannot focus their detection efforts on a single document, the passport, and concentrate their expertise on recognizing and blocking the fraudulent use of this one document. As other witnesses have testified before Congress, there are more than 240 different types of valid driver's licenses issued within the United States, and more than 50,000 different versions of birth certificates issued by U.S. States, counties, and municipalities.

Even excluding baptismal records, it would not be easy for CBP inspectors to have a passing familiarity with, let alone a working knowledge of, each of these documents. While advances in technology allow our dedicated and hardworking CBP inspectors to examine and validate documents presented for reentry, that same technology also enables the perpetrators of fraud to produce, relatively inexpensively, high-quality fraudulent documents. Forgers and counterfeiters can produce high-quality fake birth certificates and driver's licenses with off-the-shelf software programs and materials that are difficult to detect without sensitive instruments and sufficient time to examine them.

Our inspectors are also charged with detecting look-a-likes or impostors who attempt to use valid documents which belong to another person. This is one of the fastest growing phenomena in travel document abuse. Document vendors solicit genuine, unaltered documents and match them up with "look-a-likes." The Bureau of Immigration and Customs Enforcement (ICE) has developed a training program to detect impostors, which it has conducted for both U.S. and foreign immigration and border officers around the world.

Equipment costs money, and taking the time to examine thoroughly and in-depth every one of the approximately 460 million identity documents presented at our over 300 land, sea, and air ports of entry would be an enormous undertaking with potentially serious secondary effects. And, even were we to do this, this effort would only permit us to detect fraudulent documents, not, as I will discuss now, legitimately issued documents that are based on identity theft.

Identity Theft

Identity crime is the theft or misuse of an individual's personal or financial identifiers in order to facilitate other criminal activity or to gain something of value. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud. Identity crimes are frequently associated with other crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism.

The topic of identity theft is intimately connected with document fraud. As the GAO and others have shown, it is quite easy today either to obtain or produce on your home computer fraudulent identification documents, such as a driver's license or birth certificate, or to obtain valid documents issued by the appropriate authority (again, driver's licenses, social security cards, etc.) on the basis of false or fraudulent information. For example, it would be relatively easy for an individual to obtain a properly-issued State driver's license in the name of Asa Hutchinson if the individual could establish on the basis of false documents that their name was Asa Hutchinson.

Advances in technology and the explosion of e-commerce have produced enormous advantages for people around the world, and have also conferred benefits on criminals. Information collection has become a common byproduct of e-commerce transactions. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders and include both domestic and international organized criminal groups, street gangs, convicted felons, and terrorists.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

Many identity thieves use information obtained from company databases and web sites. One case investigated by the United States Secret Service, the primary DHS agency with jurisdiction over ID theft matters, involved an identity criminal accessing public documents to obtain the social security numbers of military officers. In some cases, the

information obtained is in the public domain while in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

Just last week, for example, the U.S. Attorney's Office in the Eastern District of Virginia indicted two senior partners of the Fairfax, Virginia law firm Lee & Baker who are alleged to have filed over 50 fraudulent labor certificates for Korean immigrants, who used the bogus documents to obtain green cards to remain illegally in the United States. The arrests and indictments culminated a two-year undercover investigation by federal and local authorities. For those who mistakenly believe that this type of crime does not pay, the immigrants paid $10,000 to $50,000 to obtain the fraudulent employment certifications that were filed with the Labor Departments in Virginia and Maryland.

Identity crime affects all types of Americans, regardless of age, gender, national origin, or race. Victims include restaurant workers, telephone repair technicians and police officers, to corporate and government executives, celebrities and high-ranking military officers.

Of course, and of most relevance to this hearing, fraudulent "breeder" documents obtained through identity theft can then be used to obtain genuine documents from Departments of Motor Vehicles, the Social Security Administration, and elsewhere. These legitimately issued documents can –and are – subsequently used to obtain government services and benefits and to gain reentry into the United States. There is no technology available to CBP inspectors – and none that I am aware of that exists anywhere – that would enable an inspector to determine that a legitimately issued document was actually based on a false breeder document presented to another government agency.

How DHS is Addressing the Problem

DHS and BTS are actively addressing these issues to make it harder for individuals – especially terrorists – to slip into the U.S. using fraudulent documents and to pursue identity thieves and those who use false breeder documents. We also vigorously investigate cases involving the use of fraudulent documents and cooperate with other federal, state, and local governmental entities, as well as the private sector, to heighten awareness and to reduce our vulnerabilities.

DHS uses a combination of advance information about individuals entering the U.S., pre-screening, registration systems such as the US-VISIT and National Security Entry-Exit Registration System (NSEERS), and advanced technology, including the use of biometric information that will be incorporated into our US VISIT entry-exit system.

One Face at the Border

Training CBP inspectors to recognize fraudulent documents is another important step, and one that BTS takes very seriously.

Just one week ago, Secretary Ridge announced that DHS will unify the border inspection process under one Customs and Border Protection Officer, an officer cross-trained to address immigration, customs, and agricultural inspection needs. We will have one face in one uniform -- a single officer trained for primary inspection as well as how to determine who needs to go through secondary inspections.

And since we know that Al Qaeda is interested in entering our ports illegally, this officer -- now trained in all three areas of inspection and armed with the best intelligence we have -- improves our ability to spot and stop terrorists quickly and keep them out. We have already recruited our first group of CBP officers, who will be trained throughout this fall. For DHS, this is another significant step toward our efforts to retool where it makes sense and create efficiencies and unity around a single mission.

All CBP inspectors will receive our most current training on identifying fraudulent and altered documents. CBP secondary inspectors will receive more advanced training, and BTS will continue to maintain the world-class excellence of the ICE Forensic Document Lab (FDL), that was previously housed at the INS.

ICE Resources

The sole mission of the FDL, a fully-accredited crime laboratory, is to detect and deter domestic and international travel and identity document fraud, and the FDL has developed an unparalleled expertise in the area of domestic and international travel and identity fraud.

The ICE FDL maintains a collection of exemplar documents, including birth certificates, passports, and driver's licenses to differentiate valid documents from fraudulent ones. The FDL provides real-time assistance to field personnel in identifying fraudulent documents, produces and broadly distributes Document Intelligence Alerts (high quality photographic bulletins), develops and presents training programs in the detection of fraudulent documents, and works with other Federal, state, local agencies, and foreign governments to promote common efforts to combat international document fraud.

I have brought two samples of these ICE FDL alerts and I commend them to the Members of this Committee. These alerts present, in a clear and simple format, particular features to look for in order to determine whether particular types of documents are fraudulent or counterfeit.

One alert discusses stolen blank Philippine Passports and the other concerns counterfeit Iraqi "N" series passports that were available for purchase in Turkey for about $500. The

alerts highlight how to distinguish immediately between the genuine and counterfeit document.

The FDL has on file intelligence reports of over 100,000 stolen blank, genuine, passports. These passports pose a serious potential threat to national security since they are genuine documents. The FDL has developed a reference guide that contains very precise information on the issuance process of passports and country specific intelligence information. The guide is extremely useful in identifying individuals in possession of these stolen passports.

ICE also operates a Law Enforcement Support Center in Vermont to assist state and local law enforcement officers who have questions about identification assessments during traffic stops. In addition, ICE operates units to link enforcement and intelligence resources with adjudication officers from BCIS who must make determinations about documents that they are presented for adjudication.

In addition to the work of the FDL, ICE law enforcement agents investigate cases of documents and benefits fraud. ICE has joined the U.S. Attorney's Office in the Eastern District of Virginia in a pilot project to investigate and prosecute large immigration, visa, and identification document frauds. The task force includes the participation of the FBI, Social Security Administration, IRS-Criminal Investigation, Department of State, Department of Labor, U.S. Postal Inspection Service, Virginia DMV, and the Fairfax County Police Department.

ICE investigators have logged hundreds of thousands of hours working on counterfeit document related investigations. The primary focus of these cases is to deter, disrupt, and dismantle major criminal enterprises operating not only in the United States, but in source and transit countries as well. The cases often entail long-term, complex investigations that frequently involve our international partners.

Operation Card Shark

I would also like to share the preliminary results of ICE's ongoing investigation, here in Washington, D.C., known as *Operation Card Shark*. *Card Shark* focuses on the street sale of counterfeit documents in the Adams Morgan area. Although the investigation continues, four document mills have already been closed resulting in the seizure of close to 2,000 documents with an estimated total street value of $155,000. 50 aliens have been taken into custody – 30 have been removed from the U.S. and 15 have been prosecuted.

On July 15th, one of the primary targets of this operation was sentenced in U.S. District Court to a total of 52 months in prison for his role as a kingpin in the counterfeit document-manufacturing ring.

Card Shark has disrupted the activity of three significant organizations that operate on the North side of Columbia Road and the return of Pigeon Park to the residents of Adams Morgan.

I look forward to sharing more such successes with you in the months ahead.

US-VISIT

US-VISIT is a crucial new border security and enforcement tool that will capture point of Entry and Exit information by visitors to the United States. This system will be capable of using information, coupled with biometric identifiers, such as photographs and fingerprints - to create an electronic check-in/check-out system for people who come to the United States to work or to study or visit. US-VISIT will also provide a useful tool to law enforcement to find those visitors who overstay or otherwise violate the terms of their visas and will allow us to lock-in an individual's identity, what those in the field call "positive identification" when the individual registers with US-VISIT.

By January 1, 2004, when a foreign visitor flies into one of our international airports or arrives at a U.S. seaport, the visitor's travel documents will be scanned.

Through US-VISIT, all border officers at air and some sea ports of entry will have the capability to access and review the visa information, including the photograph, during a visa holder's entry into the United States. This will enable the border officers to verify the visa photograph with the passport photograph and the individual of the visa holder during their inspection for entry into the United States. Additionally, border officers will capture biometric data to verify and lock-in a visa holder's identity. The US-VISIT system will compare the captured fingerprint against a fingerprint watch list. This will be an enhancement to the existing name check or biographical lookout check.

Prior to departure, the visa holder will have their identity verified at a self-service departure station located at air or seaports. This tells the Department of Homeland Security if that person entered legally or may have stayed illegally as some of the 9/11 terrorists did. Currently, there is no way to know when or even if our visitors leave - but under US VISIT, that will change.

On any subsequent trip to the United States, the visa holder will have their identity confirmed upon arrival and departure. Therefore, the US-VISIT program will have the capability to capture biometrics, confirm the identity of travelers, and search against both a biographical and biometric watch list to prevent document fraud, identity theft, and unauthorized travelers from entering the United States.

All of this information will become part of a foreign visitor's ongoing travel record, so their correct information can follow them wherever they go. The information will be made available to inspectors, agents, consular officials and others with a true need to know.

Mr. Chairman, we should all be clear on my next point. Good information does not threaten immigration. Quite the contrary. The more certain we are about someone's

status, the less likely we are to make a mistake that would jeopardize their status - or our safety.

NSEERS

The NSEERS program requires certain nonimmigrant aliens from designated countries to be fingerprinted, interviewed, and photographed by CBP at our ports of entry at the time they are applying for admission to the United States. In addition, other aliens who are identified from intelligence sources or who match certain pre-existing criteria determined by the Attorney General or Secretary of State may also be enrolled in NSEERS.

NSEERS helps to secure our borders, by intercepting terrorists and criminals at our ports of entry, identifying aliens who deviate from their stated purposes once they enter the U.S., and identifying aliens who have overstayed their visas and are in the country illegally. DHS officers have made every effort to minimize the inconvenience for those individuals required to register, with an average processing time of just 18 minutes.

The NSEERS registration process enables DHS to verify that an alien is living where he said he would live, and doing what he said he would do while in the United States, and to ensure that he is not violating our immigration laws.

During the enrollment process, specific biographic information, itineraries and addresses are collected. If aliens remain in the U.S. for longer than 30 days, they must return to a DHS office to confirm their address and activities in the United States. Registrants must also complete a departure check when they leave the country.

CBP Data Bases

CBP has developed the Image Storage Retrieval System (ISRS), a web based system that provides users at over 40 ports of entry with access to the biographical image sets (photographs, fingerprints and signature) used to create government issued identity documents issued by DHS. These include Alien Registration Cards (I-551s), Employment Authorization Documents), Advance Parole for Adjustment of Status forms issued by BCIS Service Centers, and Refugee travel documents. This tool allows for immediate identity verification resulting in the detection of possible fraud while facilitating the inspection of the legitimate traveler. DHS hopes to roll-out this system to all ports of entry in the next fiscal year.

Identity Theft

DHS is also working hard to reduce the incidence of identity theft, and the Secret Service is leading this effort on behalf of the Department.

This summer, the Secret Service developed and distributed to state and local law enforcement agencies throughout the United States an Identity Crime Video/CD-ROM. The CD-ROM I am holding contains over 50 investigative and victim assistance

resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM contains a short video that can be shown to police officers at their roll call meetings and discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police.

The Secret Service has authorized law enforcement agencies to make as many copies of the CD-ROM as they wish so that the agencies can distribute this resource to their officers to use in identity crime investigations.

The Secret Service is also training state and local law enforcement agencies to prevent identity theft the old fashioned way. In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, the Secret Service has hosted Identity Crime training seminars for law enforcement officers in New York, Chicago, Seattle, Dallas, Las Vegas, Washington D.C., Phoenix, Richmond, and Iowa, Mr. Chairman. The Secret Service has additional seminars planned for San Antonio, Texas next month, Orlando, Florida in November, and San Diego, California. These training seminars focus on providing local and state law enforcement officers with tools and resources that they can immediately put to use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

Collaboration

DHS and BTS are also collaborating with others in both the government and in the private sector to combat and address these important issues. We have worked closely with the Department of State on visa issuance issues and obtaining access to the Consolidated Consular Database. My staff has met several times with representatives of the Social Security Administration (SSA) to discuss issues of mutual concern and to explore how to reduce the instances of the misuse of social security numbers.

ICE has also worked cooperatively with the SSA for a number of years through the Systematic Alien Verification for Entitlements (SAVE) Program. The SAVE program enables Federal, state, and local government agencies to obtain immigration status information to determine an applicant or recipient's eligibility for many public benefits. The SAVE Program also administers employment verification pilot programs that enable employers quickly and easily to verify the work authorization of newly hired employees.

Current SAVE participants include the SSA; National Aeronautics and Space Administration (NASA); the Department of Defense Manpower Data Center; Arizona County Health Care Cost Containment; the California and Wyoming Departments of Motor Vehicles; the New Jersey Department of Law and Public Safety, Division of

Gaming Enforcement; the Mohegan Tribal Gaming Commission; and the Texas Department of Health, Asbestos Licensing Program.

The Secret Service has worked closely with the American Association of Motor Vehicle Administrators (AAMVA) to develop minimum and uniform standards for U.S. driver's licenses. I understand, for example, Mr. Chairman, that there are still four states that do not require a photograph on their state's driver's license, which, obviously, makes that document easier to use in a fraudulent manner.

Secret Service representatives work closely with the private sector on a number of efforts, and, together with the private sector, formed the Document Security Alliance as an ad hoc working group of law enforcement and industry focused on developing standards for the improving the security and traceability of plastic identification cards.

Conclusion

In sum, Mr. Chairman, DHS and BTS recognizes the enormity of the problems that we face, and we are working actively to improve our ability to detect fraudulent identification documents and to keep criminals and potential terrorists from obtaining these documents in the first place.