Statement for the Record

Senate Committee on Finance
"Homeland Security and Terrorism Threat From Document Fraud, Identity Theft and Social Security Number Misuse"
September 9, 2003, 10:00 AM
Dirksen Senate Office Building, Room 215

John S. Pistole
Federal Bureau of Investigation
Acting Assistant Director, Counterterrorism Division

Good morning Chairman Grassley and members of the Committee. On behalf of the Federal Bureau of Investigation (FBI), I would like to thank the Committee for affording us the opportunity to participate in this forum and comment on the use of identity theft, document fraud, and social security number misuse and the potential nexus to terrorism.

Unfortunately, last week's *Washington Times* article regarding three Virginia men who filed numerous fraudulent labor certificates on behalf of Korean immigrants, who then used the bogus documents to obtain green cards to remain illegally in the US, is not something totally unheard of by Americans today. One of the defendants in this case used a fake social security account number to obtain credit cards, bank accounts and a driver's license. The Federal Trade Commission, just last week, released the first large government-sponsored survey on identity theft and stated the problem was far worse than officials had believed. Last year, identity theft cost consumers more than $5 billion in expenses, while costing banks and other businesses $48 billion.

As this Committee is well aware, the FBI, along with other federal law enforcement agencies, investigates and prosecutes individuals who use the identities of others to carry out violations of federal criminal law. These violations include bank fraud, credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, computer crimes, and fugitive cases.

These crimes carried out using a stolen identity makes the investigation of the offenses much more complicated. The use of a stolen identity enhances the chances of success in the commission of almost all financial crimes. The stolen identity provides a cloak of anonymity for the subject while the groundwork is laid to carry out the crime. This includes the rental of mail drops, post office boxes, apartments, office space, vehicles, and storage lockers as well as the activation of pagers, cellular telephones, and various utility services.

Identity theft is not new to law enforcement. For decades fugitives have changed identities to avoid capture and check forgers have assumed the identity of others to negotiate stolen or counterfeit checks. What is new today is the pervasiveness of the problem. The Federal Bureau of Investigation does not view identity theft as a separate and distinct crime problem. Rather, it sees identity theft as a component of many types of crimes which we investigate.

Advances in computer hardware and software along with the growth of the Internet has significantly increased the role that identity theft plays in crime. For example, the skill and time needed to produce high-quality counterfeit documents has been reduced to the point that nearly anyone can be an expert. The same multimedia software used by professional graphic artists is now being used by criminals and terrorists alike. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents. The tremendous growth of the Internet, the accessability it provides to such an immense audience coupled with the anonymity it allows result in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme. This is particularly true with identity theft related crimes. Computer intrusions into the databases of credit card companies, financial institutions, on-line businesses, etc. to obtain credit card or other identification information for individuals have launched countless identity theft related crimes.

The impact is greater than just the loss of money or property. As the victims of identity theft well know, it is a particularly invasive crime that causes immeasurable damage to the

victim's good name and reputation in the community; damage that is not easily remedied. The threat is made graver by the fact that terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.

For example, an Al-Qa'ida terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc. Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan, Afghanistan, etc.

While the 9/11 hijackers did not utilize fraudulent identification, they did obtain US identification cards in their names. These are "legitimate" identification cards, but they are not issued by any state or federal agency. Some of the vendors the hijackers received these cards from were involved in fraudulent identification cases--they were subsequently charged and arrested. Some of the hijackers did apply for, and receive, legitimate state identification cards and Driver's Licenses.

The FBI has seen other examples of document and identification fraud in our investigations related to terrorism, to include: 1) the April 2003 arrest of William Joseph Krar in Tyler, Texas. Krar is the subject of a fraudulent identification matter, which was initiated in August 2002 based upon information developed following the delivery of a package of fake identification cards to the wrong address. The package, which contained numerous false

identifications, had been mailed from Krar in Tyler, Texas to an individual in New Jersey, an admitted member of the New Jersey Militia. The identities included a Defense Intelligence Agency identification, a United Nations Observer Badge and a Federal concealed weapons permit; 2) Top Ten Most Wanted fugitive Clayton Lee Waagner was found to have in his possession fraudulent US Marshal's badges and a significant amount of equipment for making fraudulent identification cards, in addition to bomb making materials and large amounts of currency; and 3) The investigation of the bombing of the Oklahoma City Murrah Federal Building was a collaborative effort between by the FBI and many other federal, state, and local law enforcement agencies. The evidence developed and presented in court led to the convictions of both Timothy McVeigh and Terry Nichols by two separate juries of their peers. McVeigh and Nichols, like others planning to commit a criminal act, utilized aliases. McVeigh was also known to utilize fraudulent identification.

Investigation and interviews of detainees have included the following instances of fraudulent documents and use of false identification related to terrorism matters: 1) A Pakistani detainee who served as a doctor and guard for the Taliban was detained at JFK for attempting to enter US on a forged passport; 2) An Iraqi detainee purchased a false Moroccan passport for approximately $150.00 in US currency, and used it to enter Turkey where he was arrested; 3) An Algerian detainee requested asylum in Canada after entering that country on a false passport; 4) A Yemeni detainee acquired a false Yemeni passport and was able to get a Pakistani visa; and 5) An Algerian detainee obtained a French passport in an alias name and used it to travel to London. The cost for this false passport was 3,000 French Francs.

The FBI has implemented a number of initiatives to address the various fraud schemes being utilized by terrorists to fund their terrorist activities. One involves targeting fraud schemes being committed by loosely organized groups to conduct criminal activity with a nexus to terrorist financing. The FBI has identified a number of such groups made up of members of varying ethnic backgrounds which are engaged in widespread fraud activity. Members of these groups may not themselves be terrorists, but proceeds from their criminal fraud schemes have

directly or indirectly been used to fund terrorist activity and/or terrorist groups. By way of example, the terrorist groups have siphoned off portions of proceeds being sent back to the country from which members of the particular group emigrated. We believe that targeting this type of activity and pursuing the links to terrorist financing will likely result in the identification and dismantlement of previously unknown terrorist cells. Prior to 9/11, this type of terrorist financing often avoided law enforcement scrutiny. No longer. The FBI will leave no stone unturned in our mission to cut off the financial lifeblood of terrorists.

Another initiative has been the development of a multi-phase project that seeks to identify potential terrorist related individuals through Social Security Number misusage analysis. The FBI, through its Terrorist Financing Operations Section, is taking SSNs identified through past or ongoing terrorism investigations and providing them to the Social Security Administration for authentification. Once the validity or non-validity of the number has been established, investigators look for misuse of the SSNs by checking immigration records, Department of Motor Vehicles records, and other military, government and fee-based data sources. Incidents of suspect SSN misusage are then separated according to type. Predicated investigative packages are then forwarded to the appropriate investigative and prosecutive entity for follow-up.

I again want to thank you for your invitation to speak here today, and on behalf of the FBI, look forward to working with you on this very important topic.