Testimony of

Brian Zimmer

May 2, 2007

Prepared Testimony of Brian Zimmer
Senior Associate, Kelly, Anderson & Associates
Former Senior Investigator, U.S. House of Representatives, Committee on the Judiciary
U.S. Senate Committee on the Judiciary Subcommittee on Terrorism, Technology and Homeland Security
On "Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents"
Washington, DC
May 2, 2007

Introduction

Chairman Feinstein and Ranking Member Cornyn, thank you for the opportunity to provide testimony today.

I am currently a Senior Associate at the consulting firm of Kelly, Anderson and Associates. 1 In the recent past, I had the opportunity to work with Members of Congress and jointly with the Senate staff on a number of important bills that strengthened travel document security. These included: the Enhanced Border Security and Visa Entry Reform Act of2002, Identity Theft Penalty Enhancement Act of2004, the Intelligence Reform Act of2004, and the REAL ID Act of 2005.

As the senior investigator for the House of Representative's Committee on the Judiciary from 2001 through 2006, I had the opportunity to conduct field oversight on the actual inspections of travel documents at our ports of entry.

The topic is timely, as some of the fruits of the Congressional reforms began to take shape and become realized through the administration's efforts. Individual travelers from Visa Waiver Countries who fail to meet the biometric passport requirements are, in fact, being denied entry to the U.S., when traveling without a visa. U.S. citizens are being issued the new highly secure passport with a stored digital image. If one could envision homeland security measures to prevent attacks and subversion by foreign terrorists as a patchwork quilt, it could be seen that many of the patches which were absent before 9/11 have been put in place. The premise that identity documents needs to be physically very secure, very counter resistant and issued to people only after a thorough adjudication and authentication of source identity documents is now generally accepted. At the same time, some important security patches are still missing, and others in place are only stop gap measures and need much more work. The missing "security patch" of most concern to me are the substantial non use of identity card reading technology to authenticate documents and confirm their relationship to the bearers at ports of entry and transportation terminals. Another "security patch" that continues to be put on the back burner is the application of exit controls at every port of entry.

However, these concerns are offered while recognizing that the administration is faced with funding shortfalls, and the need to balance priorities, and is often stymied in identifying practical solutions at reasonable cost. It's inherent in the changing nature of our terrorist opponents and their increasing sophistication that we will need to continue to work on closing holes in the blanket of homeland security.

Accomplishments

In my view, much has been accomplished to improve interrupt terrorist travel, and worthwhile initiatives have been undertaken by the administration to improve the security of travel documents, some of which are the result of Congressional mandates contained in the aforementioned bills.

In an appendix to my testimony, I have listed the most important federal legislation since 200 I requiring security improvements applicable to identity documents issued by federal and state agencies. Because the foundation for international travel documents issued by the United States government is highly dependent on the identity authentication adjudication by the states in the course of driver's license issuance and birth certificate issuance, the REAL ID Act is included.

Here are some of the laudable accomplishments by the administration

? US Visit - where passports are compared to the biometrics of the passport bearer, frauds are immediately identified and a reliable record is stored.

? Significant improvements in the compilation of terrorist watch lists, and of the application of these watch lists to passenger lists as filters to international air travelers' identification through passports and passenger manifests.

? Enforcement of biometric passport requirements on the countries participating in the Visa Waiver Program, along with on-site inspection of issuance processes of these same countries.

? Issuance of a new, more secure passport, with many features that will make it highly counterfeit resistant. The addition of a chip which stores the same data displayed on the photo page along with a digital photograph enables inspectors to confirm that the passport bearer is the same person to whom it was issued. The read range of several centimeters, along with shielding material and the basic access control (BAC) will help to safe guard the stored data on the chip from would be data skimmers.

? Initiation of a world wide program, working together with INTERPOL and with the European Union and Visa Waiver Program countries, to collect data about lost and stolen passports that can be employed to identity imposters and to recover passports from thieves and document brokers.

? The pending introduction of a wallet sized "PASS Card" for border crossing at the Canadian border, hopefully also with a high level of physical security built into the card.

? Establishment of federal anti counterfeiting task forces across the country. Results of their investigations are now evident with prosecutions of counterfeiting rings. These enforcement actions are equally important to security improvements in travel documents.

? A growing level of investigations and arrests by federal agents on those who sell counterfeit identity documents through the internet.

? Increased prosecutions by the Department of Justice and the U.S. Attorneys under both the Identity Theft Penalty Enhancement Act and the anti-fraud provisions of the REAL ID Act.

There has been important guidance by the Congress to the administration through enabling legislation, and there remains the need for continued oversight of the administration's efforts to complete the task list set by Congress. It is my assessment that the Administration is working hard, but finding it difficult to manage so many tasks. Homeland Security was not a priority before 9/11 and many important security improvements remain incomplete.

Cautionary Observations

U.S. Passports issued prior to the latest passport will remain in circulation and active use for border entry until 2016. There is a very strong international demand for stolen and lost U.S. passports, and it's likely the demand will become greater and the black market value higher, for the "older" passports which can be more easily altered. This means that safeguards against people using validly issued passports purchased on the fraudulent document markets needs to increase. Step one in that process needs to be a much more proactive by Customs and Border Patrol to develop techniques where an imposter carrying a passport with a "look alike" photo that closely resembles the bearer, can be identified. Machine readers are available to government purchasers that can greatly assist in such a determination.

Any major Mexican city close to the border hosts a fraudulent document market where people wishing to cross the U.S. port of entry as imposters can purchase, or sometimes "rent" U. S. passports, B1/ B2 biometric border crossing cards, and the passports of visa wavier countries. The price ranges from a few hundred dollars for a California driver's license to tens of thousands of dollars for a valid U.S. passport with a expiration date five years or more in the future, and with a photo closely comporting to the imposter. It's a rational market, following the best economic principles of supply and demand, with values based on reliability and duration of use. And all of it is dependent on the continued reliance by U.S. border inspectors on spot checks, expedited inspections, and the trained eye of the experience inspectors.

There was a time that access to these markets was restricted to those who appeared to be natives of Mexico and central American, but with the growth in other foreign visitors to Mexico on the many charter flights from around the world, anyone who has the money can make the necessary arrangements. It would be imprudent for Members of Congress to believe that the major terrorist organizations lack the money, sophistication or motivation to avail themselves of these document markets.

Beginning in 2006, there was an initiation of "100%" document inspection at nearly all of the ports of entry on the U.S. border with Canada. While the less travel ports of entry experienced little back up, the busiest ports were highly impacted and the requirement was soon relaxed.

At the majority of the ports of entry on the border with Mexico, only a small percentage of those crossing the border are subject to a "real" documents check.

This lack of document inspection is risky business. Further, no one who visits the United States and then leaves through a port of entry is subject to an exit control inspection, with or without a document check. That this situation continues nearly six years after the 9/11 attacks, and four years after our country became deeply involved with wars in Afghanistan and in Iraq, should be a major concern for the Senate. In these foreign wars, our military opponents actively practice terrorism and promote anti American terrorism on a world scale, yet we have no exist control system in place to allow us to determine whether foreign visitors are actually leaving the country.

Until border ports of entry are reconfigured to allow universal document checks, at least during periods of high security concern, and all documents are systematically confirmed, imposters entering with fraudulent, altered and stolen travel documents, such as lost and stolen U.S. passports will pass with impunity.

Primary reliance on remote data bases is not a good idea, in the absence of document inspection, whether those data bases are accessed as the result of an IC chip in a card with a secure reference number being read by an RFID scanning device or as the result of an human inspector punching a number into a computer terminal. Accessing a remote data base to confirm that an identity document presented to an inspector is a valid and authentic document, and it belongs to the person presenting it is a demonstrably valid idea. That is, remote data bases operating under a high level of system security, together with other anti fraud measure, is an excellent way to provide an additional level of safety, but it should not displace the personal confirmation of trained and experienced inspectors. The greatest risk with a central data base accessible by a reference number is that if the security of that database is significantly compromised, the individual access numbers contained on the RFID chips are likewise compromised, and the opportunity for large scale counterfeiting appears in the absence of counterfeit resistant cards.

There are reliable and secure documents used for international travel. One of the most reliable security features is the optical memory strip contained on the B1/B2 biometric border crossing cards and on Permanent Legal Resident cards. It's critical that the Department of Homeland Security continue to make border crossing cards highly physically secure, to prevent counterfeiting, and successful security features demonstrated to be counterfeit resistant should not be lightly thrown away.

An example of how easily this can happen is offered by the Employment Authorization (EAC) Card provided by CIS. Unlike the "Green Card" or Permanent Legal Resident Card, the EAC is widely counterfeited. Primary customers include scofflaw employers wishing to cover the illegal immigrant employees working for them, as evidence that the employers were "duped" by the cards. Such cards are now available, to English speaking customers, through the internet. The agency producing the EAC could have elected to employ counterfeit resistant technology to limit or potentially prevent this counterfeiting, but whether through a misguided effort to cut costs or limited vision by the program leads, elected to take the "cheap" route, leading to an insecure document. While this is not a travel document, a counterfeit EAC that looks like the real thing allows a person not lawfully present to remain undetected in the U.S., and facilitates illegal employment.

This country is at serious risk from foreign terrorists. Key priorities should be: travel documents presented at land ports of entry need to be inspected by human eyes or a highly effective automated means of inspection; all federal customs and immigration inspectors at all our ports of entry must be trained to recognize counterfeit documents; state of the are document authentication readers must be placed at primary port of entry stations to authenticate frayed or potentially alter documents; Transportation Security Administration inspectors at our airports must be trained to identify fraudulent documents, and to recognize and refuse to accept ID cards that do not meet reasonable physical security and identity adjudication standards.

Conclusion

The Administration has made important strides over the past five years toward meeting Congressional mandates addressing secure travel and identity documents. There remains a high risk that foreign terrorists will visit harm on the United States. The greatest vulnerability is in the lack of standards for both foreign travel documents and U.S. identity documents with regard to traveler inspection at airports and land borders. This risk is compounded by the absence of quality control and inspection integrity systems. The identity authentication that precedes issuance of passports by the United States is largely dependent upon source identity documents issued by the states, and that remains a serious vulnerability. Congress should support travel and identity document improvements with federal funding, including providing grants to states seeking to become compliant with the REAL ID Act.

Appendix to Testimony of Brian Zimmer, May 2, 2007
U.S. Senate Committee on the Judiciary Subcommittee on Terrorism, Technology and Homeland Security U.S. Federal Laws since 2001 which impact travel identity document Security and the need to authenticate those documents as belong to the bearers.

The following is an unofficial, informal, and probably incomplete compilation of key features and provisions of laws passed by Congress since 2001 that address identity and travel documents (both international and domestic).

It includes the USA PATRIOT Act (2001), the Enhanced Border Security and Visa Entry Reform Act of 2002 (Also Known As the Border Security Act), the Identity Theft Penalty Enhancement Act (2004), the Intelligence Reform Act (2005), and the REAL ID Act (2005).

USA PATRIOT Act

Title Three of the USA PATRIOT Act was the first step in establishing the principle that both businesses and government inspectors should be able to authenticate the identities of U.S. nationals and of foreign visitors. It identified better identification security as a key element in combating foreign terrorists entering / remaining in the U.S. It also established federal authorities to require biometrics of HAZMAT endorsement commercial drivers, which strengthened the principle of employing objective data beyond source identity documents to authenticate the holder of an identity document. It extended the principle of identity authentication for federally regulated financial enterprises as a means of identifying potential terrorists and the supporters of terrorism.

The PATRIOT Act Required a Technology Standard to Confirm Identity

403 C required the federal agencies to work through the National Institute of Standards and Technology (NIST) to develop and certify a technology standard, although the term biometric was not included, to verify the identity of foreign visitors to the U.S.

The same section also required the creation of a cross agency computer system that would have a common (biometric) set of visa holder identifiers, so that federal law enforcement officers could share law enforcement and intelligence information necessary to confirm the identity of visa applicants and those issued visas. In short, it set the basis for federal law enforcement to be able to physically identity people who had entered the country (legally). It also required that the new system would be accessible to the entire range of federal officials who actually interact directly with foreign visitors - consular officers issuing visas; border inspectors, and federal law enforcement officers such as the FBI who would investigate or otherwise need to identify aliens lawfully admitted to the United States.

Comment: This provision set the basis for common technology elements in identity management systems across federal law enforcement, which in turn affects the data available to generate identity and travel documents and the information available to authenticate the document holders with the documents.

Checking Visa Applicants' Fingerprints Against FBI Systems

SEC. 405. required a feasibility report on what level of enhancement of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) or other identification systems would be required to better identify a visa applicant, and to determine whether he/she might be wanted in connection with a criminal investigation, prior to in the United States or abroad, prior to issuing of a visa and check fingerprints at the entry or exit from the United States by that person.

Comment: this provision established the premise of US Visit, which now captures fingerprints of foreign visitors save those from Mexico and Canada, upon entry. Regrettably, there is still no such application upon exit, and therefore there is no reconciliation of records to identity visa overstays, who might easily include foreign terrorists.

Enhanced Border Security Act and Visa Entry Reform Act

Border Security Act was directed to impose requirements to find solutions to a lengthy list of homeland security problems, including especially insecure documents and inspection processes. It also set the stage for the DHS Bill and Intelligence Reform.

Expanded Pre inspection of Travelers and Anti-Fraud Measures at Foreign Airports

Section 101(c) authorized funding to train immigration officers to use the appropriate lookout databases and to monitor passenger traffic patterns, and expanded the Carrier Consultant Program. This program assigns immigration officers to assist air carriers in the detection of imposters and document fraud at those foreign airports from which a significant number of aliens arriving at US. ports of entry without valid documentation departed, but where no pre inspection station currently exists.

Adjudication and Authentication of foreign documents presented by visa applicants

Section 101(d) directed the Secretary of State to, implement enhanced security measures for the review of visa applicants, which inevitably but not specifically includes the identity documents presented by them.

Imposing a penalty on bearers of non machine readable passports

Section 103 sets the machine-readable visa (MRV) fee charged by the State Department at the higher of $65 or the cost of the MRV service, to be determined by the Secretary of State after conducting a study on such costs. This section also permits the Department to levy a $10 surcharge when an MRV is placed in a non-machine-readable passport.

Technology Standard Deadline for Visa Applicant Identity Authentication

Section 201 accelerates the deadlines contained in § 403(c) of the USA PATRIOT Act for the development of a technology standard to confirm the identity of visa applicants, and for the delivery to Congress of a corresponding report on this technology standard.

Visa Biographical Information at the Border

Section 301 requires making available to border immigration inspectors at ports of entry an electronic version of the aliens visa file, which allows visual comparison of the visa file to the bearer of the passport within which the Visa is contained.

One System for Visitor Inspection and Data Records

Section 302 essentially set the parameters of today's US VISIT program, requiring the establishment of an entry/exit data system at all U.S. ports of entry and consular posts; establish a database that compiles the arrival/departure data from all travel, entry and identity documents possessed by aliens; and make all security databases involved in determining the admissibility of aliens interoperable.

Machine Readable, Tamper Resistant International Travel Documents

Section 303 required the U.S. government and Visa Waiver Program participating countries to begin issuing machine-readable, tamper-resistant, travel documents with biometric identifiers no later than October 26, 2004. In addition, also by October 26, 2004, the government of each country participating in the Visa Waiver Program (VWP) was required to certify that it has a program to issue its nationals the same type of documents, and all individuals entering the U.S. under the VWP beginning on that date must present a passport meeting the above-described requirements unless the document was issued prior to that date. This section also requires the installation of biometric readers and scanners at all ports of entry by October 26, 2004. (The dates for compliance were extended by subsequent provisions, but all requirements have now been substantially met)

Establishment of National Standards for Biometric Identifiers

Section 303 also required that, within 180 days of enactment, that the Attorney General, the Secretary of State, and the National Institute of Standards and Technology (NIST) submit to Congress a comprehensive report assessing the actions that will be necessary to achieve the above technology requirements. This section also authorized funding to carry out its requirements. The result was the establishment of technology standards for fingerprints and digital facial images by NIST, which worked together with federal agencies to complete them. This was a very important first step in building the foundation for exchanging data among federal traveler and foreign visitor inspection systems, as well as with information stored in watch list repositories.

Reporting the Theft of Blank Passports

Section 307 stipulated that before a country may participate or continue to participate in the Visa Waiver Program (VWP), it must certify that it reports to the U.S. government on a timely basis the theft of blank passports. If the Department of Homeland Security and the Secretary of State jointly determine that a VWP country is not reporting the theft of blank passports, that country loses its ability to participate.

Comment: The administration needs to be working hard on an information system that delivers information about all U.S. and foreign stolen passports to the border inspectors at primary inspection stations.

Tracking System for Lost and Stolen Passports

Section 308 requires the Attorney General, in consultation with the Secretary of State, to enter stolen passport numbers into the interoperable electronic data system within 72 hours of notification of loss or theft.

Comment: The lack of progress on this requirement has to be considered a significant missed opportunity to improve homeland security.

Employment Authorization Documents (Secure IDs) for Refugees and Asylees

Section 309 provides that refugees, upon admission to the U.S., and asylees, upon a grant of asylum, must be provided with an employment authorization document that bears their fingerprint and photograph.

Comment: This remains a work in progress. Much more needs to be done here to raise the quality of the EADs to equivalent security of that of Permanent Legal Resident cards and to require all foreign guest workers to hold the secure cards. Currently it is an option that costs the immigrants $109. It needs to be mandatory, and the cost should be what it is required to provide a highly counterfeit resistant document.

Identity Theft Penalty Enhancement Act

The Act prescribes sentences of two years' imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations (including felonies relating to theft from employee benefit plans and various fraud and immigration offenses), and five years' imprisonment for knowingly taking such action during and in relation to specified felony violations pertaining to terrorist acts, in addition to the punishments provided for such felonies.

The Act prohibits a court from: (1) placing any person convicted of such a violation on probation; (2) reducing any sentence for the related felony to take into account the sentence imposed for such a violation; or (3) providing for concurrent terms of imprisonment for a violation of this Act and any other violation, except, in the court's discretion, an additional violation of this section.

It expanded the prior identify theft prohibition to: (1) cover possession of a means of identification of another with intent to commit specified unlawful activity; (2) increase penalties for violations; and (3) include acts of domestic terrorism within the scope of a prohibition against facilitating an act of international terrorism.

Rigorous enforcement of identity theft crimes at every level of law enforcement is extraordinarily important. As international cooperation increases to combat terrorism, al-Qaida and other terrorist organizations will increasingly turn to stolen identities to hide themselves from law enforcement.

And foreign terrorists are well aware of how to falsify identities in the United States. Five Social Security numbers associated with some of the 9/11 terrorists were "made up" and were never issued by the Social Security Administration, yet were sufficient to obtain driver's licenses and state issued identity documents from the states.

According to the official House Report on HR 173 1, one terrorist used a Social Security Number assigned to a child, and four of the terrorists were associated with multiple Social Security numbers. The same report quotes an FBI agent "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 is facilitated."2

Intelligence Reform Act

Fraudulent Document Recognition

(Sec. 7203) amends the Enhanced Border Security and Visa Entry Reform Act of2002 to require consular officer training in document fraud detection. Directs the Secretary of State, in coordination with the Secretary, to: (1) conduct a survey of each diplomatic and consular post at which visas are issued to assess the extent to which fraudulent documents are presented by visa applicants; and (2) not later than July 31, 2005, identify the posts experiencing the highest levels of fraud and place in each such post at least one full-time anti-fraud specialist unless a DHS employee with sufficient training and experience is already stationed there.

Lost, Stolen & Fraudulent Passports

(Sec. 7204) directs the President to seek international cooperation to: (1) share information on lost, stolen, and fraudulent passports and other travel documents; (2) establish and implement a real-time verification system for such documents; and (3) encourage criminalization of certain conduct that could aid terrorist travel. It also requires the President to submit annual progress reports on such efforts.

Comment: Great progress has been made through the offices of Interpol to collect the data, with over 120 countries now participating in providing data on lost and stolen passports. Interpol continues to advocate use of it's database for detecting imposters and recovering passports. The U.S. still has not met the requirements of this section, despite the success of countries like Switzerland, which now effectively uses the system's data to identity and arrest imposters. What is particularly bad about this lapse is that the inspection of persons entering with U.S. passports is not subject to any equivalent to the U.S. Visit system, which makes it relatively easy for imposters to pass through our ports of entry undetected.

Lost in Translation: Arabic & Chinese Names

(Sec. 7205) Expresses the sense of Congress that the President should seek to enter into an international agreement to modernize and improve standards for the translation of names into the Roman alphabet in order to ensure common spellings for international travel documents and name-based watch list systems.

Comment: This is a subtle but very important requirement for the federal agencies which rely on passports and visa information. The international community has standards for translations of name from native alphabets into the Roman alphabet which the English language along with Spanish, French, and major European languages. However, these rules based standards have proven to allow, and sometimes create, errors in translation. It is critical that these standards improve to facilitate correct identification of suspected terrorists whose native language requires alphabetic translation, and to avoid misidentification of people with similar names.

Visa Waiver Program Country Accountability for Secure Documents

(Sec. 7207) Requires the Secretary of State, no later than October 26, 2006, to certify which of the countries designated to participate in the visa waiver program are developing a program to issue machine readable, tamper-resistant visa documents that incorporate biometric identifiers.

Comment: Implementation and enforcement of this provision by the Department of Homeland Security has been put in place, and is a significant success story for the administration.

Biometric Passports for U.S. Citizens by 2008

(Sec. 7209) Directs the Secretary, in consultation with the Secretary of State, to implement by January 1, 2008, a plan to require biometric passports or other secure passports for all travel into the United States by U.S. citizens and by categories of individuals for whom documentation requirements were previously waived.

Comment: This requirement looks as though it will be met on time. It's important that that technology supported by facial recognition software be employed at all U.S. ports of entry, especially at land border ports of entry as soon as possible to support authentication of the digital images with the face of the person presenting the passport

Verification of Passports & Higher Standards

(Sec. 7210) Expresses the sense of Congress that the U.S. Government should: (1) exchange terrorist information with trusted allies; (2) move toward real-time verification of passports with issuing authorities; (3) where practicable, conduct passenger pre screening for flights destined for the United States; (4) work with other countries to ensure effective airport inspection regimes; and (5) work with other countries to improve passport standards.

Comment: The Department of Homeland Security together with the Department of State are proceeding with initiatives that incorporate these objectives. Congress should continue to exercise oversight to evaluate the results of these initiatives, and the current level of risk from weak passport regimes among foreign countries.

Secure Birth Certificates

(Sec. 7211) requires the Secretary of Health and Human Services (HHS) to establish minimum standards for birth certificates for use by Federal agencies for official purposes. It prohibits Federal agencies from accepting nonconforming birth certificates beginning two years after promulgation of such standards, and it requires States to certify compliance with such standards.

Comment: This requirement has not been met. In the absence of federal regulation of birth certificates, the security in some individual states is very low and there are many counterfeit or altered birth certificates in use as "breeder documents" for fraudulent identities. Under a grant by the Department of Transportation, a system which provides for electronic verification of birth certificates is now being operated in a pilot program by the National Association for Public Health Statistics and Information (NAPHSIS) and the American Association of Motor Vehicle Administrators (AAMV A). Federal funding is needed to move this pilot program into a permanent system available to all states, but the costs is very reasonable, probably in the range of $5 to $10 million per year.

More Secure Social Security Cards

(Sec. 7213) requires the Commissioner of Social Security to: (1) issue regulations restricting the issuance of multiple replacement social security cards; (2) establish minimum standards for the verification of records supporting an application for an original social security card; and (3) add death and fraud indicators to the social security number verification system. The Commissioner is required to establish an interagency task force which is to set requirements for security improvements for social security cards and numbers.

Comment: This is a very important exercise. Regrettably, until the Social Security Administration is required by specific laws to improve the physical security the card, the authentication of people's identities before issuing initial or replacement cards, and strict deadlines are set for both sets of requirements, there will likely be no meaningful security improvements by this important source of identity documents.

Restrict Use of SSNs on Cards

(Sec. 7214) Amends title II (Old-Age, Survivors and Disability Insurance) of the Social Security Act to prohibit the display of social security numbers on driver's licenses, motor vehicle registrations, or personal identification cards or the inclusion of such numbers in a magnetic strip, bar code, or other means of communication on such documents.

Comment: The states have largely changed their regulations and procedures to eliminate this practice, but it will be years before those issued prior to the Act will be removed from circulation. As long as their bearers do not choose to renew their licenses and the cards are within the issued period of reliability,

Longer Sentences for Terrorist Identity Fraud

(Sec. 7216) amends the Federal criminal code to increase penalties for fraud and related activity in connection with identification documents and information if committed to facilitate international terrorism.

Comment: This law is specifically directed at the terrorist support network here in the United States, and it will be instructive when the Department of Justice proceeds with prosecutions requesting more severe levels of penalties from the courts.

Requiring Reliable Identification Documents to Board Commercial Airlines

(Sec. 7220) requires the Secretary to propose minimum standards for identification documents required of domestic commercial airline passengers for boarding. However, standards proposed take effect only when an approval resolution is passed by the House and Senate under specified procedures and becomes law.

Comment: This law remains in limbo because the Administration has not moved forward to establish standards. Until a set of standards together with procedures is moved through Congress with an approving resolution, this common sense safeguard is not in place. Every time I move through security inspections at an airport, I'm reminded that the inspectors have no real means available to authenticate the document that I present them. Very few airport security inspectors are trained to detect a fraudulent ID card. Nor are inspectors trained to detect and reject an altered ID card. Nor are inspectors yet authorized to reject as insecure a widely counterfeited ID card, such as the Matricula Consular card issued by the Government of Mexico or the driver's licenses of some of the states.

REAL ID Act - Driver's License /Identity Document Provisions

This law is not yet in effect, with the implementing Notice of Proposed Rule Making released March 1,2007, and comments from public due by May 8, 2007. It is likely the implementing regulations will become final by the end of September, 2007. The REAL ID Act requires that a REAL ID driver's license be used for "official purposes," as defined by DHS.

In the proposed rule, DHS will limit the official purposes of a REAL ID license to those listed by Congress in the law: accessing a Federal facility; boarding Federally-regulated commercial aircraft; and entering nuclear power plants.

DHS has set minimum standards for what will appear on the face of the card, because that is required by the PL 109 -13. The proposed regulation requires each of the following on the face of REAL IDs: space available for 39 characters for full legal name; address of principal residence; digital photograph; gender; date of birth; signature, document number; and machine readable technology.

Temporary REAL IDs will need to clearly state that they are temporary.

Non-REAL IDs issued by compliant States must state on their face that they are not acceptable for Federal official purposes and be of a unique design or color that clearly distinguishes them from REAL ID licenses. The Notice of Proposed Rule Making does not require a State to collect fingerprints, iris images, or other biometric data in connection with obtaining a license.

At this stage of development, only a traditional image is required, so long as it captured with digital technology allowing it to be exchanged I authenticated with other states.

2 - D Barcode is required, and RFID Chips are not. The Machine Readable Technology specified in the NPRM is the 2-D barcode already used by 46 jurisdictions (45 States and the District of Columbia), and not used by five.

Comment: REAL ID will (eventually) change how licenses look, but the initial proposed rule does not specify precise designs or layouts of state issued licenses, or a single common layout. Greater commonality of design would greatly reduce the complexity of physical inspection, aid in detecting counterfeit and altered documents, and reduce training expense. However, DHS is undoubtedly responding to its extensive consultation with the more security conscious among the states, who have a legitimate interest in minimizing cost and protecting existing production facilities. In the absence of at least a few common design elements, the use of card reading and authentication machines with sophisticated operating software will become a standard requirement for law enforcement, and hopefully, airport inspectors.

I Among the clients of Kelly, Anderson and Associates are both government agencies and companies who have interests in secure document technology and identity document inspection. This testimony is submitted in my personal capacity.

2 Official House Report on HR 1731