Testimony of Digimarc Corporation
Before the House Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism

July 26, 2007, "Frequent Traveler Programs: Balancing Security and Commerce at our Land Borders"

Presented by Thomas Gann
Digimarc Vice President, Public Policy

Chairwoman Sanchez and Ranking Member Souder, I would like to thank you both, and your colleagues on the Subcommittee, for giving me an opportunity to present Digimarc Corporation's views on improving border security while also promoting legitimate cross border travel and commerce. As the leading supplier of government-issued citizen identity documents in North America, Digimarc is pleased to be of service to the Subcommittee.

Customs and border protection and law enforcement officers face extraordinary challenges as they try to authenticate the more than 200 forms of valid driver licenses circulating in the U.S. today through unaided visual inspection. My testimony discusses technological innovations that are available now and in use by several state governments and commercial entities to augment visual inspection of driver licenses. Such technologies, like digital watermarking, are already in broad distribution and can be used to machine authenticate U.S. driver licenses, travel documents and other modern identification documents in the immediate future. These technologies should be integrated into a flexible platform that can accommodate new innovative technologies that are developed in the future.

Digimarc and the Importance of Digital Watermarking

Digimarc (www.digimarc.com), based in Beaverton, Oregon, has supplied issuance systems for driver licenses and other government-issued credentials for nearly 50

years and is the leading supplier of government-issued IDs in North America. We produce more than two-thirds of all driver licenses issued in the U.S. and offer products and services in more than 25 other countries. Additionally, we are a trusted supplier of a global system used by an international consortium of central banks to deter digital counterfeiting of currency.

Digimarc supports U.S. states with solutions covering all aspects of ID issuance: applicant identity verification and enrollment; over-the-counter and centralized secure card production systems; design and manufacturing of the cards using advanced technologies and multiple security features; and inspection to authenticate the ID after issuance.

Additionally Digimarc pioneered a signal processing technology innovation known as "digital watermarking," which allows imperceptible digital information to be embedded in all forms of media content, including personal identification documents, financial instruments, photographs, movies, music and product packages. In identity documents digital watermarking is used to embed digital data imperceptible to the human eye within the structure of the document. Using commercially available devices such as scanners, PDAs with built-in cameras and other digital technology, it's possible to authenticate IDs and readily identify counterfeit and fraudulent documents. We believe that digital watermarking, to be discussed further later, is an important component of securing the nation's borders.

U.S. states began incorporating digital watermarking into their driver licenses in 2002 using a Digimarc product known as Digimarc® IDMarc™, and to date 20 states have adopted this security capability in their driver licenses. The list includes Iowa, Wyoming, Nebraska, New Jersey, Kansas and Massachusetts as well as key border States such as Washington, Michigan, Minnesota, Florida, Texas, Vermont and others that keep their use of the technology confidential for security reasons. By the end of the year, one out of every two driver licenses being issued will include digital watermarks, and this number is growing rapidly.

Our Insecure Borders:

Since Sept. 11, 2001, the United States Government Accountability Office (GAO) has published a number of studies that have demonstrated how insecure our borders really are. In 2003, and also as described in today's testimony, GAO officials partnered with agents of the Office of Special Investigations to develop counterfeit documents used by special agents to enter the United States from various ports of

entry from the Western Hemisphere. In GAO's most recent series of tests, 17 of 19 counterfeit driver licenses successfully presented to cross into the United States were produced by using off-the-shelf, commercially available graphics software, a computer, a scanner and a printer, and were. Our hard-working border officials were unable to detect these fakes because they do not have all the tools they need to properly verify the authenticity of these types of documents.

Visual inspection of travel documents — the key method our inspectors have today — is inadequate for a number of reasons, including the fact that there are more than 200 valid U.S. driver license formats. Only specialists, with years of training, have the skill sets needed to conduct reasonable visual inspections, and even then, visual inspection alone is not adequate to catch digital counterfeits. Our border agents do not have the necessary training or tools to inspect these documents on a day-to-day basis at ports of entry. This is made more difficult by the demands that arise from timely processing of thousands of individuals every day. Machine-authentication of the digital watermark present in many of these documents, however, would take the guess work out of determining which documents are valid and which are not.

The WHTI Initiative and the Economic Challenges of the PASS Card:

To improve the security of our borders, the Western Hemisphere Travel Initiative (WHTI), under the Department of Homeland Security (DHS), mandates that upon seeking entrance to the United States across a land border port of entry, all travelers, including U.S. citizens, present a passport, other verifiable and secure document, or combination of documents that can ensure a person's identity and citizenship. This initiative has already begun to change travel for U.S. citizens traveling between the U.S. and both Canada and Mexico.

More than 29 million people move across the U.S. / Canadian border to engage in trade and tourism each year, supporting more than $1.2 billion of daily trade between the countries. In 2004, Canadians spent $10.3 billion in the U.S., nearly $8 billion of which was spent on travel and tourism.

As only 25% of U.S. Citizens hold passports, the initial implication of WHTI was that each citizen traveling home from Canada or Mexico had to obtain a valid passport at the cost of nearly $100. To ease the financial burden, and to partly address the concerns of the business community, DHS has proposed a driver-license-like "passport lite" document called the PASS Card.

While the PASS card is a sensible approach to giving citizens an alternative to buying a passport for purposes of travel in the Western Hemisphere, a coalition of U.S. and Canadian businesses, called Business for Economic Security, Trade & Tourism (BESTT) comprised of over 60 associations and companies, believes that the PASS proposal, as currently written, will significantly reduce commerce between the US and Canada. Indeed, BESTT has cited one estimate saying the new identification requirements could cost the U.S. economy $785 million a year and the Canadian economy $1.7 billion in lost revenue due to a decline in tourism.

The coalition "opposes requiring passports for Americans and Canadians entering the U.S., and instead, urges the U.S. and Canadian government to develop another approach that would do a better job of balancing commercial and homeland security interests." BESTT has also urged both the U.S. and Canadian government to consider allowing REAL ID compliant drivers licenses to be used as border crossing cards – a concept that has real merit.

Leveraging State Investments in ID Security to Secure our Borders:

Many states have established security processes that complement and extend many of the processes employed in the current U.S. passport, or the expected PASS card. The states have made and are making major investments in their driver licenses and issuance systems to promote transportation safety, protect their citizens from identity theft and fraud, and enhance their personal security and the security of the nation – particularly since September 11. As we know, the perpetrators in the Sept. 11 terrorist attacks obtained valid driver licenses under false identities. In any security system, criminals tend to look for weak points to exploit. In these cases, the documents were genuine driver licenses obtained fraudulently. States and their suppliers are upgrading not only the documents but also the enrollment process and inspection processes to address all known weaknesses that could be exploited by criminals.

According to the National Conference of State Legislatures, the states are expecting to invest billions of dollars as they continue to enhance the security of their driver licenses in compliance with the REAL ID Act, which sets federal security standards for state-issued driver licenses and IDs. These efforts will result in a high level of security in the enrollment, issuance and inspection processes of our current driver licenses. These same processes and technologies being deployed by the states could also be used to strengthen the enrollment processes for Federal employee credentials and citizen credentials such as passports, and can be used in conjunction

with gaining citizenship certification from the Department of State for State-issued REAL ID-compliant driver licenses. These improved enrollment processes include:

- Secure in-person photo capture to protect against fraudulent photo submittal and enable downstream biometric facial recognition
- Electronic scanning and archiving of documents enabling efficient enrollment, subsequent forensic investigation of documents, and electronic transmittal as part of adjudication process
- Electronic document authentication at point of enrollment using a variety of machine readable features including digital watermarking
- Electronic applicant verification against federal and third party databases such as Social Security
- Electronic verification of applicant data against State DMV and vital record databases
- Facial and/or fingerprint recognition, both 1-to-1 and 1-to-many, to verify identity against existing biometric records
- Use of trained driver license agency personnel who are experienced in fraudulent document recognition, work with enrollment processes on an ongoing basis, and have successfully passed thorough background checks

Leveraging Existing Technologies to Secure our Borders:

As described above, proven, cost-effective technologies are commercially available today that can enable border officials to machine authenticate U.S. driver licenses and other border crossing credentials. These documents contain numerous security features such as digital watermarks, holograms, and special inks. There are software and hardware solutions available that can automatically inspect such security features and facilitate background checks via third party data bases. Digital watermarks are key in that they provide the only means of trusted authentication of a driver license in use today, and they can be read using commercially available scanners with special software.

Digital watermark-based document authentication solutions are compatible with other travel document reading efforts including the ePassport efforts. This capacity to work with an ever-evolving set of security features is essential because it ensures that government can stay ahead of terrorists and criminals who seek to use loopholes in our security systems to gain access to the U.S. Additionally, these technologies can be quickly deployed, within six to 12 months, and are efficient for the inspector to use so that citizens are not inconvenienced with long lines. And essential to success, digital watermarks do not compromise citizen privacy.

Summary of Nebraska ID Authentication Pilot Results:

The state of Nebraska provides a particularly poignant example of raising the ID security bar by deploying innovative security solutions and processes. In 2003, Nebraska was one of the first States in the country to incorporate the digital watermarking feature into its licenses.

In 2005, the Nebraska Department of Motor Vehicles conducted a pilot under a grant from the U.S. Department of Transportation to demonstrate authentication of digitally watermarked driver licenses as a means to fight ID counterfeiting, reduce the purchase of age-restricted products, such as alcohol, and enhance traffic safety. Digital watermark scanners were installed in a total of 18 point-of-sale sites, 30 office sites, and 35 law enforcement sites, and were used in "real time" for an average of 30 days. Retailers, law enforcement and DMV operators were equipped with reader devices that allowed them to verify the information printed on a driver license -- even an unfamiliar out-of-state driver license -- against the information contained in the digital watermark. By doing so, they were able to determine if a driver license was valid or not and, in the retail situations, which, if any, age-controlled products the DL holder was old enough to purchase. The scanner/reader devices proved invaluable in instantly determining whether or not the license presented was authentic, as well as validating the age of the DL holder.

At the conclusion of the pilot, Digimarc staff interviewed the users regarding their experience with and response to the digital watermarking technology. The technology was extremely well received:

- 100% of retail participants said that a valid read from the watermark gave them confidence that the DL was authentic.
- 100% of law enforcement participants using a PDA reading device had confidence that a valid read from the watermark meant the DL was authentic.
- 100% of office staff surveyed reported that they believed the device was beneficial, that it gave them confidence that the scanned ID was authentic, and that they would use it in the future.

The deployed readers continue to be used by the state, and in fact, this summer, Nebraska plans to put new Document Inspector units into production at DMVs across the State. This will arm front-office operators with the tools to inspect and positively authenticate the millions of U.S. driver licenses secured with digital watermarking (Digimarc's ID Marc). When Nebraska and other state driver licenses are presented

as proof of identity to obtain a new or renewal driver license, machine authentication will be able to validate the ID or detect fraud. The system will be effective with licenses from neighboring states such as Colorado, Iowa, Kansas and Wyoming - effectively removing the guesswork that can come with visually inspecting an out-of-state ID.

Today, more than 60% of valid driver licenses in Nebraska are secured with digital watermarking, and it is anticipated that within two years all valid Nebraska licenses in circulation will be protected by digital watermarking. Nebraska's experience – as well as that of other states such as Iowa – can serve as a model for the federal government to help make our nation's borders more secure in a timely and cost effective way. Iowa, for instance, has deployed secure card materials, digital watermarking, and many other cutting edge solutions. The state employs full time investigators to attack license and identity fraud, and has deployed advanced readers to help officials detect counterfeits.

Digimarc Document Inspector Scenario

Authenticating documents like driver licenses and IDs can be done quickly and simply with a single device that scans both sides of the document simultaneously – a device such as the Digimarc Document Inspector software that checks the validity of common ID security features, including the digital watermark. To determine if a license is genuine, an inspector would start inspecting the document by inserting it into the scanner. The software is very easy to use – the operator just hits the spacebar to initiate the scanning process. In just a few seconds, the device scans both sides of the document and the software processes the information, determining if the document is authentic for that document type and jurisdiction. The software contains a regularly-updated document information library that is used for this automated validation process.

The software reads the individual's demographic data from the document and displays the key data and associated analyses to the operator, which assists validation of the document and card holder. This entire process produces a valid rating in seconds, displaying "green" clearly on the screen if the license is valid and red if it is suspect. With such a process, operators can easily see if the document passed inspection - enabling them to focus on the individual, rather than the document. In a typical border crossing scenario, if a red indicator appears, the card holder would be sent to secondary inspection where an investigator could use the digital watermark and other features or databases to pursue the fraud.

Digital watermarks can also be read and authenticated on travel document scanners, like the kind used to read passports. Software such as Digimarc's software is able to draw on the pattern matching library of such a scanner and its multi-spectral light inspection authenticate the watermark and check additional security features visible only when illuminated in UV or IR light. This is a more expensive solution, but one that can validate not just driver licenses and IDs, but travel documents like passports and foreign ID cards.

The Document Inspector closes the loop on the secure ID lifecycle by providing an easy, reliable way to instantly authenticate IDs after issuance. Border inspectors can immediately validate the document using the digital watermark and other data and features present on the license. Visible features, like 2D barcodes and others, can be altered, but when linked to a second feature that is imperceptible to the human eye, counterfeiting becomes extremely difficult, if not impossible. After scanning, Document Inspector provides a quick pass/fail reading and keeps lines moving.

Document Inspector is fast and easy-to-use. An operator can authenticate a document with confidence in just a few seconds. The software is hardware independent, working seamlessly with a variety of best-of-breed hardware and software components, and provides a simple user interface to eliminate the guess work associated with visual inspection.

Table 1 summarizes the Document Inspector features and benefits.

Table 1 Digimarc Document Inspector Features and Benefits

Features	Benefits
Extensive document database that is updated regularly	• Standardizes authentication practices • Gives agents more confidence • Keeps the knowledge base up to date without the need for additional training
Fast, easy authentication results	• A clear red/green indicator of authentication evaluation • Multiple visual cues to the result • Ability to see the details if further investigation is necessary

Standards-based technology	• Allows for integration with external systems • Keeps deployment/investment costs low • Provides clear technology path

In summary Digimarc Document Inspector is a document authentication solution that features:

- A system that offers fast document authentication to ensure citizens are not inconvenienced or slowed down by the process.
- Authentication of the most comprehensive set of security features used in driver licenses

Cost Estimates of Deploying Readily Available Technologies:

We don't have access to all of the government information, including technology integration, human resource, and third-party database expenses, to offer a precise estimate of what it would cost the federal government to deploy these readily available technologies to help secure our borders. However, we respectfully suggest that the Committee request that the Congressional Budget Office or the Office of Management and Budget conduct such a study.

It is our understanding that the number of Northern and Southern land border points of entry are:

	Inbound Passenger Lanes	Inbound Cargo Lanes	Pedestrian Lanes	Total Lanes
Northern Land Border POEs	278	121	24	423
Southern Land Border POEs	224	72	86	382
Total	502	193	110	805

Our own rough estimate of the cost - based on our experience and market research studies - of deploying the necessary software and hardware in an estimated 805 lanes to cover all immigration land border lanes, including cargo and shoulder lanes is under $50 million. This would equip each lane to machine validate driver licenses and other common travel documents. Covering the Northern border lanes, assuming 423, the cost is approximately $26 million. If we wanted to add any type of remote database interface to this system such as cross referencing watch list databases or consolidating the number of transactions etc., we would add an additional $10 million to our baseline cost estimates.

These cost estimates do not include the cost to the States of deploying machine-readable security features, nor do they capture the expense to the States of improving a large number of their security programs such as their enrollment processes. But these requirements have already been mandated by the REAL ID Act and the States are already working out how to pay for compliance with this Act. In any case, if our cost estimates are roughly in the ball park, this would be a small price to pay to quickly improve the security of our borders.

New Technologies: A Smart Card Capability to Enhance the Security of Travel Documents:

Some months ago, DHS signed a Memorandum of Understanding with the state of Washington to authorize a pilot of a drivers license that would be enable to be used as a PASS card. The department has also made it known that it welcomes similar proposals from other states as a thoughtful approach to augmenting the current PASS program. We believe the Department is on the right track by giving states and their citizens another way to comply with the requirements of the PASS card.

One key component of the PASS plan is to include a micro-chip in the card to enable it to either run on the same technology infrastructure of the new passport that is being rolled out, or to introduce a remote reading capability – the ability to determine a few minutes before citizens actually cross the border whether their credentials are valid. This capability, the government believes, will help ensure that citizens can move quickly across the border while ensuring that high level of security is maintained.

Recently, Washington DOL and DHS have agreed to run an initiative that allows the Enhanced Driver License (EDL) to be used as an alternative travel document to re-enter the United States through sea and land border crossings. Digimarc will supply Washington DOL with applicant enrollment and screening solutions as well as

production of the RFID-enabled EDL. Recent state legislation authorizes the use of enhanced driver licenses, issued on proof of citizenship, identity and residency, as a WHTI alternative document to a passport for re-entry into the United States. The new Washington licenses will cost $40.

Washington's enhanced driver license system will employ Digimarc applicant screening solutions to verify an applicant's identity documents, data such as name and address, and facial biometrics to ensure that only one license is issued to one legitimate card holder.

Digimarc launched its chip-enabled driver license solution last year in anticipation of States' needs for new applications of the driver license. The Digimarc enhanced driver license for Washington will include RFID technology that is compatible with the DHS Western Hemisphere Travel Initiative program. This will offer a convenient and cost-effective option for citizens to carry a single credential that meets their driving, identity, and land and sea border crossing needs.

The Enhanced Driver License itself will carry traditional security features found on the current Washington driver license, including digital watermarking, as well as new features including an RFID chip and a "Machine Readable Zone" (MRZ) that is compatible with travel document readers.

The Washington initiative will leverage a number of market leading Digimarc driver license products and services to provide a high level of security throughout the process, including:

- Document authentication of "foundation documents" used to obtain an enhanced driver license;
- Applicant data verification that will be used by interviewers to confirm the data presented by applicants, including name, address or date of birth;
- 1:many facial recognition-based biometrics to screen out duplicate ID fraud, which is part of the gated issuance process to coordinate the back-end screening process and release the enhanced driver licenses to production; and
- Production of the enhanced driver license at a secure, centralized facility.

Public Policy Recommendations

We recommend that as the Federal government rolls out its next procurement to enhance border security, it purchase technologies that are both forward and backward compatible. The Federal government should deploy capabilities to machine verify the authenticity of U.S. driver licenses at the border, including reading and authenticating the digital watermark. Over time, these readers could be upgraded to accommodate enhancements being made to driver licenses and other identity documents from both the U.S. and Canada, and also other from other Western Hemisphere countries as deemed appropriate by the Department of Homeland Security and the Department of State. These technology solutions are scalable, having the capacity to integrate new technologies that will be developed in the future to ensure that criminals and terrorists are always challenged to defeat ever higher levels of security.

Every border crossing official must be able to do machine-readable verification of driver licenses, processing the covert machine readable features in documents that are presented at the border. In addition to putting stationary readers at all border crossing stations, mobile readers should also be deployed to ensure that agents can do rapid and secure screening of driver licenses and/or travel documents. This will help ensure that transit times are not unduly affected. All of these technologies exist today and are proven and could be readily deployed if the funds were available.

The REAL ID law requires the States to add a machine-readable feature to their driver licenses. Given that digital watermarking has become a de facto standard for driver license authentication, we recommend that the federal government require or encourage all States to adopt digital watermarking technology in addition to other appropriate machine-readable security features to comply with the requirements of this law so that national standard authentication will be realized. We also urge that digital watermarking be added as an additional security feature to all border crossing credentials.

The REAL ID law will help States meet the security challenges of the 21st century by ensuring that they deploy best-of-breed, end-to-end security systems. However, the states have estimated that the cost of implementing the Real ID Law will be $13 Billion. The states have also asked the federal government to fund the $1 Billion in start up costs that the states have identified. We urge Congress help the states pay for these start up investments in hardware, software and card materials.

Finally, we applaud the Administration for approving the Washington state pilot and urge that additional pilots be approved. These pilots can test the viability of leveraging state issued drivers' licenses to promote secure and efficient cross border travel. We believe that these pilots, as they prove successful, can form the basis for a program that will allow as many states as possible to issue dual use driver's licenses. This approach would leverage the significant investments in ID security that the States have already -- and will continue to make, in the coming years. Such a policy will also leverage the existing ID systems that the Canadian Provinces have already deployed. The opportunity for both the United States and Canada to develop a collaborative approach should not be missed.

Conclusion

In conclusion, I would like to thank Chairwoman Sanchez and ranking Member Souder for giving me the opportunity to appear before your Subcommittee on behalf of Digimarc Corporation. The States have been pressing forward with important security upgrades within the limits of their budgets and mandates. More will need to be done as States drive to comply with the REAL ID law. It makes sense, therefore, for the federal government to leverage these significant investments to help secure our borders, and at the same time, save taxpayers money and time in obtaining identification credentials. Digimarc Corporation, along with other suppliers and the many of the issuers that we serve stand ready to do all we can to support the government's objective of enhancing the security of our homeland.

*Additional information on digital watermarking

Digital watermarking complements other authentication techniques such as the pattern matching and multi-spectral analyses found in passport and travel document scanners. Digital watermarking technology is compatible with and can enhance the security of passports, smartcards and other travel documents such as the proposed PASS Card. Digimarc broadly licenses digital watermarking technologies to many other vendors for supply of digital watermarking enhanced solutions for a variety of security purposes.

Deployment of digital watermark reading is aligned with the published security strategies of the Department of Homeland Security and the Department of State, and is a recommended feature of the Document Security Alliance and an approved optional feature of the HSPD-12 PIV-2 standard, which calls for enhancing the identification and authentication of federal employees and contractors. Digital

watermarks provide positive document authentication, age verification, cross-jurisdictional authentication, and forensic capabilities.