

May I See
Your Papers Please?



Supplement Packet to:

The Real ID Act of 2005: Real Tyranny Against Americans

Compiled by the National Veterans Committee on Constitutional Affairs

Copyright information contained in original document

Prepared as an educational tool for the use of State Legislators

Considering implementing the Real ID Act of 2005 at their state level.

Updated: October 17, 2007

Contents

“Introduction” By Aaron Bolinger, Legislative Director, NVCCA.	1
Dear Colleague Letter of Rep. Sam Rohrer, R-128, Penna. House of Representatives	3
“Real ID Act: America’s Next National Security Crisis” By Sam Rohrer	5
“The Real ID Act of 2005” by Mark Lerner	6
“Constitutional Controversies: Will Gun Owners Say Goodbye to the Second Amendment?” By Sam Rohrer	9
“Medical Microchip for People May Cause Cancer” By the Associated Press.	10
“L-1 Identity Solutions Adds Industry Experts”	16
L-1 Identity Solutions Board of Directors.	18
“Vissage Awarded Over \$48 Million in Contracts” By Business Wire.	23
“L3 Founder LaPenta To Put A New Face on Viisage” By Boston Business Journal.	26
“Opposing Sides Work Together to Derail Real ID” By Sam Rohrer.	27
“Biometric Fact Sheet” By STOP REAL ID Coalition.	28
“A Christian Perspective on Real ID & Biometrics” By STOP REAL ID Coalition.	32
Model Legislation: “Bodily Integrity Act” by CAISPAN.	39
Model Legislation: “Pennsylvania H.B. 1351” (with amendments).	40

INTRODUCTION

by: Aaron Bolinger

This document is intended as a supplement to the original book published under the same title. In the time since publication, much more information has come to light about the subject of biometrics, human/animal chipping, and the interlocking links between business and government who are promoting “Real ID.” This packet is not designed to replace the other document, but to enhance it.

The information from both these documents is also being assembled into a single new book. If you have only this supplement, please acquire a part one original at www.lulu.com/bolinger.

This supplement provides a simple way to update the original, and make sure the new information about the Real ID Act of 2005 is made available to state legislators who are considering either implementation, or rejecting implementation, within their state.

State legislators must carefully weigh this new evidence against the pressure being brought to bear by federal officials. The decision to implement Real ID represents a several century slide BACKWARDS where individual liberties are concerned. Personal and religious freedoms protected by constitutional provisions are virtually and practically erased by federal legislation such as Real ID. What it purports to require of both states and individuals marks the end of the separation of powers as the past centuries have known.

One thing that should make nearly any legislator upset is being lied to. The evidence available (for legislators who do their homework) confirms that the biometrics industry has indeed lied about both the accuracy of biometrics devices, and their alleged “safety.” Review this information carefully, and notice that this supplemental packet contains a new model piece of legislation entitled the “Bodily Integrity Act.” This bill would prohibit the non-consensual implantation of any biometric “chip” or device in a human being. It further prohibits “coercion” (employment considerations, etc.) of any individual to receive such a device. The need for this Bodily Integrity Act, *in addition to* the other model legislation contained in the first part of the book, will become apparent.

Another situation that is an immediate cause for alarm among public officials is the *appearance* of severe conflicts of interest between former high-ranking government officials and the corporations set to profit greatly from the implementation of Real ID. Indeed, the leading company supplying “advanced” driver’s license technology to state governments (L-1 Identity Solutions) openly boasts of the number of “insiders” who are part of their corporate structure (see the L-1 Information herein). When one finds the Department of Homeland Security as the primary driving force behind implementing Real ID, and former top officials therein (such as Admiral James Loy) in chief stockholder/board of directors positions within L-1 Identity Solutions, any thinking person would immediately wonder with great marvel. To find former CIA chief George Tenet also a director and chief shareholder within L-1 makes the situation even more interesting, as it is obvious the database of information being stockpiled via Real ID will eventually fall into the hands of these federal investigation/intelligence agencies. So not only will the CIA/DHS gain information on mostly law-abiding citizens of the United States, but the former directors thereof will financially profit by states procuring L-1 equipment.

State legislators know the dangers of being both inside of government (in policy positions) and taking money from the corporate world who supply government contracts. As one state legislator remarked when reviewing this information, the “classic definition of fascism” is evident. “This is not about security,” he said. “It is about making money.”

Are we kidding? No. Some of that evidence is presented in this supplemental packet. Read the material, check out the authenticity of the information, dig deeper, and consider implementing the Real ID “package” proposed by the federal government with this knowledge in mind. The only sane answer appears to be the passage of state laws prohibiting the implementation of Real ID within our states, and providing protections that prevent the general public from being harassed into accepting dangerous biometric devices in or on their bodies. As the public becomes ever more aware of these realities, the

authority, necessity and propriety of implementing Real ID becomes greater and greater in doubt.

The main problem in some states is that their Motor Vehicle Departments have been already awarding contracts to L-1 (and others) prior to any formal policy supporting it passing the legislature. The state assemblies involved MUST make *informed* decisions to implement Real ID. (See the L-1 press release of June 13, 2006 where they boast of over \$48 million already awarded by the states of Pennsylvania, Wisconsin, Arkansas, and Maryland.) In those states, an obvious *reversal* of direction will be needed by the policy-makers, along with un-doing any contracts already awarded. This of course has embarrassing implications toward the executive branch in those states. Add several layers of “politics” to the equation and one can see the subject must be approached thoughtfully.

The NVCCA is concerned about these realities, but our primary function is to make the information about Real ID known. The chips will necessarily fall as they must in states that have failed to follow up or investigate before taking some action toward implementing Real ID.

I remain at the disposal of anyone needing assistance, and take my responsibility seriously to those who took up arms in defense of America – our veterans. On behalf of the NVCCA, I remain,

Respectfully,

Aaron Bolinger, Legislative Director

SAMUEL E. ROHRER, MEMBER
128TH LEGISLATIVE DISTRICT
ROOM 45 EAST WING
PO BOX 202128
HARRISBURG, PA 17120-2128
PHONE: (717) 787-8550
FAX: (717) 783-7862
srohrer@pahousegop.com

DISTRICT OFFICE:
29 VILLAGE CENTER DRIVE, SUITE A7
READING, PA 19607
PHONE: (610) 775-5130
FAX: (610) 775-3736
www.samrohrer.com



House of Representatives

COMMONWEALTH OF PENNSYLVANIA
HARRISBURG

COMMITTEES

GAME & FISHERIES,
REPUBLICAN CHAIRMAN
EDUCATION
SPEAKER'S COMMISSION
ON LEGISLATIVE REFORM

CAUCUSES

EAST CENTRAL CAUCUS
PA LEGISLATIVE SPORTSMEN

October 16, 2007

Members of the State Legislature

Dear Colleague,

I write today on a matter of grave importance to you and the citizens of your state, as well as all citizens of this great country—the Real ID Act of 2005

This act requires all 50 states to move to a federally approved driver's license containing machine-readable technology, personal information and photograph; and link the information contained in that license to a national identification database. Every licensed driver in this country, currently about 245 million individuals, would have to go *personally* to their local Department of Motor Vehicles with their certified source documents (i.e., birth certificate, Social Security card) and apply for a Real ID. Any citizen who did not comply would not be able to board a plane, enter a federal building, or obtain services from the federal government.

The Real ID driver's license was originally required to be implemented by all of the 50 states by May of 2008. However, the controversies surrounding Real ID have resulted in compliance being postponed until 2013. An ever-growing number of states have passed legislation, or are considering legislation, stipulating that they will not comply with, participate in, or fund the implementation of the Real ID Act.

Dozens of groups from every part of the political spectrum oppose Real ID, including the National Governors Association, the National Conference of State Legislatures, the American Association of Motor Vehicle Administrators (the association of state DMVs), Gun Owners of America and the ACLU.

Objections most notably include the costs, the loss of individual liberties and the commandeering of state government rights by the federal government. The Department of Homeland Security (DHS) estimates the cost of the **unfunded mandate** to be \$23.1 billion, with \$14.6 billion of this to fall to the states. The machine-readable technology required by the act is not clearly defined. It could, in the future, include Radio Frequency Identity Chips (RFID) which have already been incorporated into our United State Passports. These chips would allow a citizen to be tracked from a distance without his, or her, knowledge. The act also gives DHS the authority to require biometric identifiers like fingerprints or retinal scans. Can you imagine the fodder that one, national database containing so much of our private information will be to identity thieves?

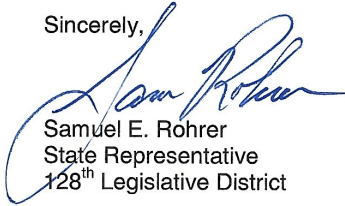
Perhaps from a legislative perspective, such a demand from the federal government is clearly unconstitutional and poses a serious challenge to state sovereignty. Simply stated, neither Congress, the President, nor any bureaucracy of government possesses the constitutional authority to mandate such sweeping regulations on the citizens of our various states.

October 16, 2007

Here in Pennsylvania, I have introduced House Bill 1351, which sends a strong message to the federal government that Pennsylvania will not participate in Real ID. This bill, which already has significant bipartisan support, provides in part that neither the Governor nor any Commonwealth agency shall participate in compliance with any provision of the federal REAL ID Act of 2005 until the US Department of Homeland Security guarantees that such implementation will not compromise the economic privacy or biometric data of any resident of Pennsylvania. The legislation also states that the provisions of the federal Real ID Act of 2005 are not to be implemented in Pennsylvania until all costs have been met through federal funding. Finally, under this legislation, either the Governor or the Attorney General may file an action in a court of competent jurisdiction to challenge the constitutionality or legality of the REAL ID Act of 2005.

Although the pretense of the Real ID Act is to strengthen anti-terrorism and anti-illegal immigration activities, the violations of individual and states' rights supersede this claim. I ask you to stand with us here in Pennsylvania and other state legislatures in opposing this intrusion by the federal government into our state's rights and the individual rights of our citizens.

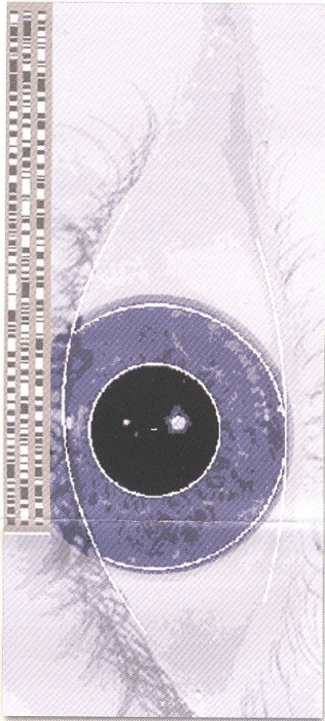
Sincerely,



Samuel E. Rohrer
State Representative
128th Legislative District

SER/bjj

REAL ID Act: America's Next National Security Crisis



Proponents of REAL ID insist that establishing a uniform national identification system will provide America with the most effective defense against terrorism that the world has ever seen, deliver unbeatable illegal immigration control and eradicate completely the crime of identity theft.

Unfortunately, the facts regarding this specific proposal lead to a completely different conclusion:

- **License to Terrorize:** Make no mistake about it, confidential information will be compromised through the implementation of a national identity system. For example, Social Security numbers, license plate numbers and driver's license numbers do absolutely nothing to provide an accurate terrorist profile or determine evil intent and can be adapted, counterfeited and reproduced by domestic or international terrorists to complete their deadly missions. Because REAL ID standardizes licenses, it makes it easier to duplicate licenses.
- **State-of-the-Art Passport for Illegal Aliens:** Similarly, some national security experts advancing REAL ID as the "silver bullet solution" to end America's illegal immigration epidemic refuse to acknowledge or put into practice real world solutions that would actually fulfill the federal government's constitutional obligation to secure our nation's borders against foreign invaders. Producing fraudulent identification is a major key to success for any illegal immigrant who wants to avoid detection in the United States. Rather than forcing individual states to spend hundreds of millions of dollars in revenue to implement REAL ID, taxpayer dollars would be much better spent on other programs, such as building border fences or training local police to identify and prosecute illegal aliens.
- **More Identity Theft, You Bet:** Computer and security experts around the globe have repeatedly gone on record stating that creating a single REAL ID standard will lead to even more rampant identity and asset theft. Centralizing personal, financial and medical data on one single REAL ID card guarantees convenient "one-stop shopping" for any technologically-savvy identity thieves.

Reagan Is Still Right About REAL ID

The July 9, 2007, edition of *The New American* magazine reported that President Ronald Reagan opposed then U.S. Attorney General William French's proposal to implement a "perfectly harmless" national ID card system as well as a second cabinet member's proposal to "tattoo a number on each American's forearm."

According to former White House domestic policy adviser, Martin Anderson, the "Great Communicator" responded "My God, that's the mark of the beast," signaling an abrupt end to the national ID card debate during the Reagan years.

Unfortunately, due to the bipartisan endorsement by both Republicans and Democrats at the federal level, the REAL ID monster is again alive and well in the 21st century with the very real capability to unleash a fully-functional and expandable national identity system which could be able to track the movements and activities of each and every law-abiding American citizen.



Extract from "Rohrer Sounds Warning Against REAL ID Act"

A flyer published by Rep. Sam Rohrer, District 128, Penna. House of Representatives,
and the Republican Caucus of Pennsylvania.

THE REAL ID ACT 2005

by: Mark Lerner

The concept of the Real ID Act goes back over 20 years ago (1986) to the passing of the Commercial Motor Vehicle Safety Act. Included in the Act were provisions for the use of biometrics. Since that time both the ICAO (International Civil Aviation Organization) and the AAMVA (American Association of Motor Vehicle Administrators), two international organizations, have been promoting the use of biometrics, the creation of linked databases, and the sharing of information globally.

Before going on it is important that people know what the definition of biometrics is. There are many but they all come down to this:

biometric: Any specific and uniquely identifiable physical human characteristic, *e.g.*, of the retina, iris, facial recognition, acoustic spectrum of the voice (*i.e.*, voiceprint), fingerprint(s), handwriting, pattern of finger, lengths, *etc.*, that may be used to validate the identity of an individual.

As is so often the case it is not necessarily one reason for a law (Real ID Act) being passed. The biometric industry as a whole has been losing money year in and year out for many years, including the years prior to 9/11. The industry saw 9/11 as an opportunity to recoup their losses. Immediately after 9/11 the industry invested more money on Research and Development and marketing. The losses mounted for the industry when large federal contracts did not come as anticipated. In the winter of 2002 it was obvious to most that we were headed on a war track. By the time the war in Iraq started shares of biometric company stock's were plummeting. The industry was desperate as it became apparent money was going to be diverted from Homeland Security to the war effort. The result was the biometric industry as a whole was making wild, unsubstantiated claims of success regarding the capabilities of their technology. Testing parameters were put in place to achieve desired results. Both the industry and the government knew but concealed that controlled testing in a laboratory environment was not and is not indicative of real life applications. The hope was one day the technology would catch up with the "hype". It didn't at the time and still has not even as of today.

It is noteworthy that many people have been incorrectly identified as a person other than who they actually are as a result of the use of biometrics. In September 2007 a federal district court judge ruled on issues related to the Patriot Act. The judge ruled that provisions of the Patriot Act are unconstitutional. This in itself is important but also is the fact the person who brought the suit was himself wrongly identified through the use of fingerprint technology as being someone other than who he was. In 2002 the largest facial recognition company in the United States announced they had achieved 90% accuracy results using their technology in a test sponsored by the U.S. government. Sounds pretty good until you know they intentionally deceived the public concerning the results. The fact is they achieved nowhere near 90% accuracy for the entire testing period. A Freedom of Information request was done and the actual results the company achieved were roughly 1/2 as good as they company claimed. The technology was NOT accurate over 50% of the time. That did not matter to the Chairman of the Board of the Company. He wrote a Letter to the Editor informing all in the public that read the letter that the technology did achieve 90% results and we would all be much safer with the use of the technology. You can decide for yourself what you would call such a person that would make such false claims. I am not talking about a company that makes washing machines; I am talking about a company who wanted it's technology to be used to better protect us all. The sad news is that technology and this company are being used by many agencies and departments in the federal government, including DHS, to protect us all.

The same company, Viisage Technology now known as L1 Identity Solutions, the largest biometrics/document company in the United States, went so far as to provide material information concerning guidance, acquisitions and even at least one contract to a brokerage house. That brokerage house used that information for their own and it's clients advantage. This was information that was not released to other investors at the same time. This was done apparently in order that the company's stock would be purchased by the brokerage house and it's clients which would result in the share price of the stock going up. That would and did lead to a secondary offering being completed by the biometrics company which raised many million's of dollars for the company. Noteworthy is the fact that while this was taking place the Chairman of the Board of the company controlled/owned nearly 33% of the stock.

While this was playing out two international organizations, AAMVA and ICAO, recognized an opportunity to push their own agendas forward. The ICAO, a U.N. organization, task was and is to monitor

commercial airline traffic internationally. The use of biometrics would allow the agency not just to compile more information about travelers but also to match people's identity/names with their biometric/facial characteristics. ICAO documents reveal that the ICAO was pushing for the use of biometrics long before 9/11. The AAMVA, which one would think by name alone is an American organization that works with U.S. motor vehicle administrators, is much more and not an American organization at all. As it's own web site reveals on it's homepage, it is an international organization that serves law enforcement. We must put an end to international organizations having such wide influence on U.S. policy and laws. In the Real ID Act NPRM (Notice of Proposed Rulemaking) there is constant reference in footnotes, you know those things at the bottom of the pages in small print that nobody reads to the AAMVA and the ICAO.

One could reasonably debate who or what is behind this international effort to collect, maintain and share all private citizen's of the world most sensitive/personal information. The fact is it doesn't matter. What does matter is this invasion of people's privacy and attack on people's "right's" was and is taking place. It is not a new concept to use CCTV (Close Circuit Television) for surveillance applications. In the United Kingdom, CCTV was and is being used to capture an image of people who were in the vicinity of a criminal events or terrorist attacks. The technology was only helpful after an event took place. Now with claimed advances in facial recognition technology CCTV can and will be used to identify people and track them before an "event" takes place. Combining this technology with the information shared globally in databases, government's will be able to try to forecast who is potentially going to be guilty or complicit in terrorist or criminal activity and who is not. The story is actually much worse. Technology is being developed to identify a potential "bad" person by the way or in the manner they walk, their gait. Add in data mining technology and all pretense of privacy and individual rights are lost. People are presumed guilty and must prove their innocence.

Data mining technology and the largest provider of information gleaned from data mining have constantly been the subject of both federal and international investigations. ChoicePoint located in Georgia has been the subject of investigations and lawsuits. Just this year, 2007, ChoicePoint settled a suit that specified that the company or one of it's current subsidiaries released private citizen's personal/sensitive information without consent. Noteworthy is there is a direct connection between ChoicePoint and L1 Identity Solutions. Not only do they have contracts with the same governments but they also have direct links between the members of their respective Board of Directors.

Many news articles, books and television reports report that we are all, the world's population, connected to one another through as few as six people. This premise or theory is well documented. It's validity is not the issue. The issue is if that is the belief that law enforcement and intelligence agencies hold then theoretically if not practically we all are associated with criminals or terrorists. This is why the burden has shifted to people having to prove they are innocent otherwise they are thought of as being guilty. That is a high burden or threshold to meet. One must provide any and all information about themselves in order to "try" and remove themselves from being considered as a "bad" person or associated with a "bad" person. Today people that are suspected of being terrorists or terrorist sympathizers are put on a no fly list. It takes many years to get a name/person removed from the list. It is not a leap at all to consider with the Real ID Act and the use of all the technologies discussed in this document that a person could be wrongly identified as being a terrorist or terrorist supporter. Should that happen to you or anyone else they would not be able to acquire the Real ID driver's license. This would mean that life as you or they knew it would be over until the years passed that it would take to clear your/their name. This of course ASSUMES that at some point DHS would get it right and realize you are not a threat.

As if all this is not suspect enough the picture is much bleaker once one looks under the surface. As a result of worldwide acceptance of common or standardized identification, the issuer of that identification through default controls the citizenry of the world. Without the identification one is not able to travel or participate in commerce. We see this in the Real ID Act. A U.S. citizen cannot fly commercially, enter a federal building or other things without the Real ID. Financial institutions and retailers will insist on this new identification, the Real ID license, before allowing us to participate in the buying and selling of goods and services. Freedom and privacy will be just words that no longer exist in the "real" world. To complicate issues further congress has left the door wide open for DHS to be able to modify for what purposes the Real ID license will be required.

Those with religious beliefs that conflict with the requirements to obtain the Real ID are being told they must accept the ground rules, thus change their religious beliefs rather than the law being changed. In our country state's rights or sovereignty will be lost forever. What has always been a state's right which was to issue identification and share information as needed with other state's will now be in the hands of the federal government and to some extent in the hands of the international community. If a person or an

entire state decided to opt out of Real ID a practical example of this control would be the person in that state who has an issue about their Social Security or Medicare. Without the Real ID license that person would not be able to enter a federal building to address their concerns. Although the DHS (Department of Homeland Security) states the Real ID Act is voluntary it clearly is not. Without said identification a person could not exist in our society. By default the program becomes mandatory. It is also worth noting that DHS claims they will not be linked directly into this massive database that will result when all states open up their databases to one another. Whether you believe DHS or not on this point the fact is DHS already has this right, the right to any and all information contained in state DMV databases. The 1994 Driver's Privacy Protection Act provides DHS with the right to the information. No warrant is needed. They are not even required to show probable cause before the information is gathered.

Should Americans knowingly or not knowingly forfeit their right's, they may believe they have nothing to hide then presumably they have nothing to fear. That is not the case. Biometrics don't work as advertised and innocent people have been wrongly identified as being someone other than who they are. The Habeas Corpus doctrine has been stricken in matters related to terrorism. An American citizen can be whisked away to Guantanamo and declared an enemy combatant with virtually no rights.

This is not a democrat versus republican issue. Yes, there are those that would like to make it just that but only to divert our attention from the Act itself and what the implications are. On one hand we have republicans that are deeply invested in the biometrics industry and on the other hand we have democrats that originally headed up the biometric companies. They had and have a mutual interest and that is money. In addition we have another set of players and they are the corporations who favor initiatives such as WHTI (Western Hemisphere Travel Initiative) and SPP (Security and Prosperity Initiative) otherwise known as the NAU (North American Union). These are initiatives designed for only one reason and that is to improve commerce. There are those that would claim these programs improve or increase national security but the reality is they create seamless borders and threaten our national security.

The result or consequences of the Real ID Act are not the sole proprietorship of one person, one party, one organization or one corporate entity. Each of the aforementioned has their own motivations but at the end of the day the one thing we should all agree on is the Real ID Act destroys the liberties and freedom so many before us have given the ultimate sacrifice for. The Real ID Act must be stopped now. Once the enrollment process takes place, information is collected, databases are created and linked it will be too late to undo the harm. Information will no longer be able to be retrieved and deleted no more than emails can be successfully removed by hitting the delete key on a keyboard. Just like the emails, the information contained in Real ID and similar databases will exist somewhere on servers, hard drives etc..

There is the issue of identity theft. Identity theft is the fastest growing crime in the United States. When, as the Real ID Act mandates, state's DMV databases are linked the prize for identity thieves is exponentially multiplied if they, the identity thieves, are successful in compromising any one state's DMV database because all DMV databases will be linked. It is worth noting there have been instances in the past that either as a result of hacking or "inside" access, state DMV databases have been compromised. The increased value of the prize now will only lead to one result which is more attempts to compromise databases. One should always keep in mind that social security numbers are now stored in state DMV databases.

Finally, I ask that you appreciate that with this international sharing of information there is another issue. We are being asked to trust that other countries will exercise the same due diligence we expect our country to exercise before identification documents such as the Real ID license are issued. Many countries around the world have had their government's infiltrated not just by terrorists or terrorist sympathizers but also by narco-terrorists. It is significant that recently it has been discovered that many people of Middle Eastern decent have moved to Mexico and applied for and received legal names changes resulting in their names now appearing Hispanic rather than Arabic. These same people have received Mexican identification with the name changes. Our border control and customs people were not aware of this issue until just recently. We have no way of knowing just how many of these people used that valid identification to enter the United States. The point is we must not leave the national security of the United States in the hands of the countries. Also consider that we are being asked to trust conceivably twenty something year old employees in government offices located around the world to insure that breeder documents that are presented in those countries to obtain identification documents such as passports, are in fact authentic. I don't know about you but I do not feel safe knowing that a 21 year old working in a Saudi Arabian government office is being charged with the responsibility of determining whether a birth certificate or some other type of breeder document being presented is authentic. That employee must and will make that determination before issuing that person a document such as a passport. With regard to 9/11 we have already witnessed just how poorly a job the Saudi's did at

authenticating breeder documents. This circumstance is not unique to Saudi Arabia and could potentially play out in any other country in the world. Here is a novel idea: We should accept more responsibility for protecting our own borders and leave less responsibility in the hands of other countries to protect our homeland. Whatever a person's position is on the immigration issue, we should all agree that our borders need and should be more secure than they are.

Some are guilty or to blame: All are responsible. Each American is responsible for protecting the rights we have been afforded under our constitution. We can ponder who is to blame down the road but right now we must stop this insanity and attack on our freedom.

One may think I have no basis for much of what I describe or I am making assumptions that can't be supported. Before one draws that conclusion they should know 1) I am a prior biometrics industry confidant who had relationships with many senior people including the President's and Chairmen of the Board's of biometric companies. 2) I sat in on many conferences that revolved around policy issues related to the use of biometrics. 3) I was in direct/personal contact with many people in law enforcement, our intelligence community and our military. 4) I am a strong advocate for national security and believe we face a real threat from Islamic extremists. Further I am prepared to support every allegation/claim I make. I will and can provide sources for the information I provide and in addition can provide evidence of the wrongdoing in the biometrics industry that I charge. That evidence comes in many forms including emails, other documents and tape recordings. Statements are provided by the same people who were working at the companies while the wrongdoing was taking place. I have turned over this material to many people in our government. This took place in August of this year, 2007. Myself and others are waiting, albeit not too patiently for the result of that information/evidence being turned over. Please appreciate that in 2005 I turned over much of the same evidence to a federal agency. I was asked to respect a confidentiality request. I did so for over a year before I went public. I could no longer wait in good conscience while the investigation continued. To this day I have never heard the results of that investigation or if in fact it was ever completed.

There are alternatives to the Real ID Act that would in fact strengthen our national security and protect our liberties. That is a discussion for another time. Suffice it to say I and others are not opposed to tamper proof licenses, low resolution photographs that could not be used for facial recognition technology and the authentication of breeder documents (birth certificates, etc.) by direct contact between the issuing agency of the identification document and the agency that issued the breeder document. We are strongly opposed to the linking of state databases.

Constitutional Controversies: Will Gun Owners Say Goodbye to the Second Amendment?

As Republican Chairman of the House Game and Fisheries Committee, I am deeply concerned about how the rights of law-abiding gun owners will be impacted if the REAL ID Act ever takes effect.

The Second Amendment clearly states that our right to keep and bear arms shall not be infringed upon. Thus, it is safe to say that Benjamin Franklin, Thomas Jefferson, James Madison and the rest of our nation's founding fathers would not even consider carrying around a biometric REAL ID card that would allow the federal government to instantly track their activities and whereabouts.

If Ben Franklin walked into his local gun shop, today, to purchase a hunting rifle, he would fill out the standard 4473 registration form and display his driver's license. However, under the REAL ID scenario, this routine transaction would significantly change.

Rather than simply reviewing and copying down some basic information from Mr. Franklin's driver's license, the store clerk would run his new RFID-equipped REAL ID card through a scanner so that his purchase was automatically recorded into both the state and national driver's license registries.

Keep in mind, it is presently illegal for both state and federal governments to maintain any type of registry of legal firearm purchases. However, the REAL ID Act will provide the Department of Homeland Security, Federal Bureau of Alcohol, Tobacco and Firearms, Federal Bureau of Investigation, and state and local police with an open invitation to not only "peek" inside and locate every recently purchased firearm in any law-abiding gun owner's gun cabinet, but to also access his or her most personal and confidential information.

Because the swiping of your driver's license would be required, the collecting and maintaining of your private information is very possible. Whether you are purchasing shells or bullets for hunting, recreational target shooting or self defense, the store will scan your REAL ID card, and your purchase will be permanently registered in the federal government's national driver's license registry.

In essence, the federal government could also have the ability to limit the number of guns and amount of ammunition you are allowed to purchase or own. If you try to buy more than the government's approved ration, your purchase would be instantly denied by the national database.



Would Daniel Boone Support REAL ID? House Republican Game and Fisheries Committee Chairman Rohrer fires an authentic Pennsylvania Long Rifle at the Keystone State's only live flintlock firing range located at the Daniel Boone Homestead in Exeter Township.

In most cases, the names and confidential information of violent intruders will not show up in any database, including those made possible by the REAL ID Act, because of one very obvious and logical reason: Criminals, illegal aliens and terrorists obtain their firearms illegally.

Just like all other types of gun control mandates, whenever the government is not properly enforcing the laws that already exist to curtail violent crime, it is nothing short of an unconstitutional infringement to place additional restrictions on law-abiding citizens whose only desire is to defend their lives, their loved ones and their property.



Medical microchip for people may cause cancer

Company didn't tell public of decade-old studies tying device to rat tumors



Proponents say microchips, when implanted in people, offer security and medical identification benefits. Detractors warn that they're tied to tumors and that abuse of the chips will eliminate personal privacy in the digital age.

When the U.S. [Food and Drug Administration](#) approved implanting microchips in humans, the manufacturer said it would save lives, letting doctors scan the tiny transponders to access patients' medical records almost instantly. The FDA found "reasonable assurance" the device was safe, and a sub-agency even called it one of 2005's top "innovative technologies."

But neither the company nor the regulators publicly mentioned this: A series of veterinary and toxicology studies, dating to the mid-1990s, stated that chip implants had "induced" malignant tumors in some lab mice and rats.

"The transponders were the cause of the tumors," said Keith Johnson, a retired toxicologic pathologist, explaining in a phone interview the findings of a 1996 study he led at the Dow Chemical Co. in Midland, Mich.

Leading cancer specialists reviewed the research for The Associated Press and, while cautioning that animal test results do not necessarily apply to humans, said the findings troubled them. Some said they would not allow family members to receive implants, and all urged further research before the glass-encased transponders are widely implanted in people.

To date, about 2,000 of the so-called radio frequency identification, or RFID, devices have been implanted in humans worldwide, according to VeriChip Corp. The company, which sees a target market of 45 million Americans for its medical monitoring chips, insists the devices are safe, as does its parent company, Applied Digital Solutions, of Delray Beach, Fla.

"We stand by our implantable products which have been approved by the FDA and/or other U.S. regulatory authorities," Scott Silverman, VeriChip Corp. chairman and chief executive officer, said in a written response to AP questions.

The company was “not aware of any studies that have resulted in malignant tumors in laboratory rats, mice and certainly not dogs or cats,” but he added that millions of domestic pets have been implanted with microchips, without reports of significant problems.

“In fact, for more than 15 years we have used our encapsulated glass transponders with FDA approved anti-migration caps and received no complaints regarding malignant tumors caused by our product.”

The FDA also stands by its approval of the technology.

Awareness questioned

Did the agency know of the tumor findings before approving the chip implants? The FDA declined repeated AP requests to specify what studies it reviewed.

The FDA is overseen by the [Department of Health and Human Services](#), which, at the time of VeriChip’s approval, was headed by Tommy Thompson. Two weeks after the device’s approval was formally announced on Jan. 10, 2005, Thompson left his Cabinet post, and within five months was a board member of VeriChip Corp. and Applied Digital Solutions. He was compensated in cash and stock options.

Thompson, until recently a candidate for the 2008 Republican presidential nomination, says he had no personal relationship with the company as the VeriChip was being evaluated, nor did he play any role in FDA’s approval process of the RFID tag.

“I didn’t even know VeriChip before I stepped down from the Department of Health and Human Services,” he said in a telephone interview.

Also making no mention of the findings on animal tumors was a June report by the ethics committee of the [American Medical Association](#), which touted the benefits of implantable RFID devices.

Had committee members reviewed the literature on cancer in chipped animals?

No, said Dr. Steven Stack, an AMA board member with knowledge of the committee’s review.

Was the AMA aware of the studies?

No, he said.

Published in veterinary and toxicology journals between 1996 and 2006, the studies found that lab mice and rats injected with microchips sometimes developed subcutaneous “sarcomas” — [malignant tumors](#), most of them encasing the implants.

- A 1998 study in Ridgefield, Conn., of 177 mice reported cancer incidence to be slightly higher than 10 percent — a result the researchers described as “surprising.”
- A 2006 study in France detected tumors in 4.1 percent of 1,260 microchipped mice. This was one of six studies in which the scientists did not set out to find microchip-induced cancer but noticed the growths incidentally. They were testing compounds on behalf of chemical and pharmaceutical companies; but they ruled out the compounds as the tumors’ cause. Because researchers only noted the most obvious tumors, the French study said, “These incidences may therefore slightly underestimate the true occurrence” of cancer.

- In 1997, a study in Germany found cancers in 1 percent of 4,279 chipped mice. The tumors “are clearly due to the implanted microchips,” the authors wrote.

Caveats accompanied the findings. “Blind leaps from the detection of tumors to the prediction of human health risk should be avoided,” one study cautioned. Also, because none of the studies had a control group of animals that did not get chips, the normal rate of tumors cannot be determined and compared to the rate with chips implanted.

Still, after reviewing the research, specialists at some pre-eminent cancer institutions said the findings raised red flags.

- “There’s no way in the world, having read this information, that I would have one of those chips implanted in my skin, or in one of my family members,” said Dr. Robert Benezra, head of the Cancer Biology Genetics Program at the Memorial Sloan-Kettering Cancer Center in New York.

Before microchips are implanted on a large scale in humans, he said, testing should be done on larger animals, such as dogs or monkeys. “I mean, these are bad diseases. They are life-threatening. And given the preliminary animal data, it looks to me that there’s definitely cause for concern.”

Dr. George Demetri, director of the Center for Sarcoma and Bone Oncology at the Dana-Farber Cancer Institute in Boston, agreed. Even though the tumor incidences were “reasonably small,” in his view, the research underscored “certainly real risks” in RFID implants.

In humans, sarcomas, which strike connective tissues, can range from the highly curable to “tumors that are incredibly aggressive and can kill people in three to six months,” he said.

‘Some reason to be concerned’

At the Jackson Laboratory in Maine, a leader in mouse genetics research and the initiation of cancer, Dr. Oded Foreman, a forensic pathologist, also reviewed the studies at the AP’s request.

At first he was skeptical, suggesting that chemicals administered in some of the studies could have caused the cancers and skewed the results. But he took a different view after seeing that control mice, which received no chemicals, also developed the cancers. “That might be a little hint that something real is happening here,” he said. He, too, recommended further study, using mice, dogs or non-human primates.

Dr. Cheryl London, a veterinarian oncologist at Ohio State University, noted: “It’s much easier to [cause cancer](#) in mice than it is in people. So it may be that what you’re seeing in mice represents an exaggerated phenomenon of what may occur in people.”

Tens of thousands of dogs have been chipped, she said, and veterinary pathologists haven’t reported outbreaks of related sarcomas in the area of the neck, where canine implants are often done. (Published reports detailing malignant tumors in two chipped dogs turned up in AP’s four-month examination of research on chips and health. In one dog, the researchers said cancer appeared linked to the presence of the embedded chip; in the other, the cancer’s cause was uncertain.)

Nonetheless, London saw a need for a 20-year study of chipped canines “to see if you have a biological effect.” Dr. Chand Khanna, a veterinary oncologist at the [National Cancer Institute](#), also backed such a study, saying current evidence “does suggest some reason to be concerned about tumor formations.”

Meanwhile, the animal study findings should be disclosed to anyone considering a chip implant, the cancer specialists agreed.

To date, however, that hasn’t happened.

The product that VeriChip Corp. won approval for use in humans is an electronic capsule the size of two grains of rice. Generally, it is implanted with a syringe into an anesthetized portion of the upper arm.

When prompted by an electromagnetic scanner, the chip transmits a unique code. With the code, hospital staff can go on the Internet and access a patient’s medical profile that is maintained in a database by VeriChip Corp. for an annual fee.

VeriChip Corp., whose parent company has been marketing radio tags for animals for more than a decade, sees an initial market of diabetics and people with heart conditions or Alzheimer’s disease, according to a Securities and Exchange Commission filing.

The company is spending millions to assemble a national network of hospitals equipped to scan chipped patients.

But in its SEC filings, product labels and press releases, VeriChip Corp. has not mentioned the existence of research linking embedded transponders to tumors in test animals.

When [the FDA](#) approved the device, it noted some VeriChip risks: The capsules could migrate around the body, making them difficult to extract; they might interfere with defibrillators, or be incompatible with MRI scans, causing burns. While also warning that the chips could cause “adverse tissue reaction,” FDA made no reference to malignant growths in animal studies.

Did the agency review literature on microchip implants and animal cancer?

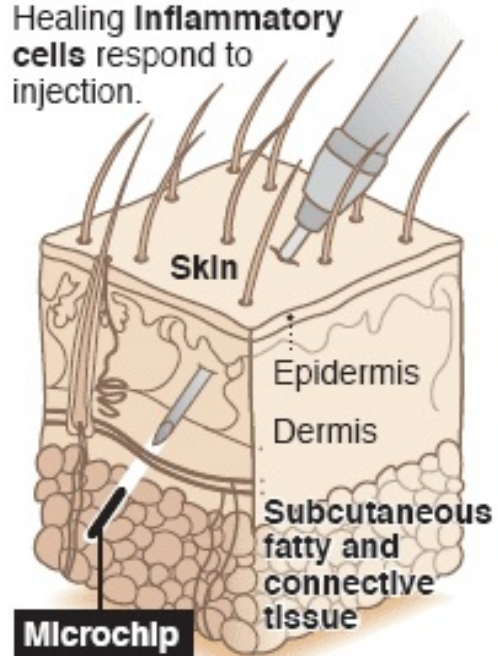
Adverse reaction to chipping a dog

A recent study says a dog’s cancerous tumor which developed after a microchip injection in 2004, is similar to tumors previously seen in cats after vaccination injections.

How microchips may induce malignant tumors

Veterinarians have found irritations, inflammation and wounds are promoters of tumor development.

Healing Inflammatory cells respond to injection.



Overzealous inflammatory cells may produce compounds that enhance the growth of malignant tumors at **microchip** site.

SOURCES: Veterinary Pathology; AP
The Complete Book of Dog Care

Dr. Katherine Albrecht, a privacy advocate and RFID expert, asked shortly after VeriChip's approval what evidence the agency had reviewed. When FDA declined to provide information, she filed a Freedom of Information Act request. More than a year later, she received a letter stating there were no documents matching her request.

"The public relies on the FDA to evaluate all the data and make sure the devices it approves are safe," she says, "but if they're not doing that, who's covering our backs?"

Protecting trade secrets

Late last year, Albrecht unearthed at the Harvard medical library three studies noting cancerous tumors in some chipped mice and rats, plus a reference in another study to a chipped dog with a tumor. She forwarded them to the AP, which subsequently found three additional mice studies with similar findings, plus another report of a chipped dog with a tumor.

Asked if it had taken these studies into account, the FDA said VeriChip documents were being kept confidential to protect trade secrets. After AP filed a FOIA request, the FDA made available for a phone interview Anthony Watson, who was in charge of the VeriChip approval process.

"At the time we reviewed this, I don't remember seeing anything like that," he said of animal studies linking microchips to cancer. A literature search "didn't turn up anything that would be of concern."

In general, Watson said, companies are expected to provide safety-and-effectiveness data during the approval process, "even if it's adverse information."

Watson added: "The few articles from the literature that did discuss adverse tissue reactions similar to those in the articles you provided, describe the responses as foreign body reactions that are typical of other implantable devices. The balance of the data provided in the submission supported approval of the device."

Another implantable device could be a pacemaker, and indeed, tumors have in some cases attached to foreign bodies inside humans. But Dr. Neil Lipman, director of the Research Animal Resource Center at Memorial Sloan-Kettering, said it's not the same. The microchip isn't like a pacemaker that's vital to keeping someone alive, he added, "so at this stage, the payoff doesn't justify the risks."

Silverman, VeriChip Corp.'s chief executive, disagreed. "Each month pet microchips reunite over 8,000 dogs and cats with their owners," he said. "We believe the VeriMed Patient Identification System will provide similar positive benefits for at-risk patients who are unable to communicate for themselves in an emergency."

And what of former HHS secretary Thompson?

When asked what role, if any, he played in VeriChip's approval, Thompson replied: "I had nothing to do with it. And if you look back at my record, you will find that there has never been any improprieties whatsoever."

FDA's Watson said: "I have no recollection of him being involved in it at all." VeriChip Corp. declined comment.

Thompson vigorously campaigned for electronic medical records and [healthcare](#) technology both as governor of Wisconsin and at HHS. While in President Bush's Cabinet, he formed a "medical

innovation” task force that worked to partner FDA with companies developing medical information technologies.

At a “Medical Innovation Summit” on Oct. 20, 2004, Lester Crawford, [the FDA’s](#) acting commissioner, thanked the secretary for getting the agency “deeply involved in the use of new information technology to help prevent medication error.” One notable example he cited: “the implantable chips and scanners of the VeriChip system our agency approved last week.”

After leaving the Cabinet and joining the company board, Thompson received options on 166,667 shares of VeriChip Corp. stock, and options on an additional 100,000 shares of stock from its [parent](#) company, Applied Digital Solutions, according to SEC records. He also received \$40,000 in cash in 2005 and again in 2006, the filings show.

The Project on Government Oversight called Thompson’s actions “unacceptable” even though they did not violate what the independent watchdog group calls weak conflict-of-interest laws.

“A decade ago, people would be embarrassed to cash in on their government connections. But now it’s like the Wild West,” said the group’s executive director, Danielle Brian.

Thompson is a partner at Akin Gump Strauss Hauer & Feld LLP, a Washington law firm that was paid \$1.2 million for legal services it provided the chip maker in 2005 and 2006, according to SEC filings.

He stepped down as a VeriChip Corp. director in March to seek the GOP presidential nomination, and records show that the company gave his campaign \$7,400 before he bowed out of the race in August.

In a TV interview while still on the board, Thompson was explaining the benefits — and the ease — of being chipped when an interviewer interrupted:

“I’m sorry, sir. Did you just say you would get one implanted in your arm?”

“Absolutely,” Thompson replied. “Without a doubt.”

“No concerns at all?”

“No.”

But to date, Thompson has yet to be chipped himself.

L-1 Identity Solutions Adds Industry Experts to Bolster Federal Government Marketing Efforts

Former Director of the Joint Interagency Task Force South for the U.S. Coast Guard and Former Deputy Assistant Secretary for Passport Services for the Department of State Join L-1

STAMFORD, Conn., May 30, 2007 (BUSINESS WIRE) -- L-1 Identity Solutions, Inc. (NYSE:ID), a leading provider of identity solutions and services, added further depth of experience and expertise to the Federal government marketing team with the addition of Rear Admiral Jeffrey J. Hathaway and Frank E. Moss. Admiral Hathaway is the former director of the Joint Interagency Task Force South for the U.S. Coast Guard and will serve as a full-time Vice President of Federal Programs for L-1, beginning June 1, 2007. Former Deputy Assistant Secretary for Passport Services for the Department of State, Frank Moss, began serving as a consultant to the L-1 Federal Program on May 1, 2007. Both individuals will leverage their extensive backgrounds in Homeland Security-related issues to develop relationships with various Federal agencies driving identity-related national and international programs.

"These individuals represent a wealth of knowledge on identity-related issues facing the public and understand how critical it is to align government agencies and programs with the best solutions available to better protect and secure our citizens," said Robert V. LaPenta, Chairman, President and CEO of L-1 Identity Solutions. "It is an honor and privilege to have Frank and Jeff join our team. We believe their contributions will have a meaningful affect on our ability to continue to deliver best-of-breed solutions and services for any Agency facing these challenges."

Coast Guard Officer Contributes Valuable Anti-Terrorism / Law Enforcement Experience and Interagency Coordination Skills

Rear Admiral Jeffrey J. Hathaway has more than 30 years of service at sea and ashore with the U.S. Coast Guard and has served as the Director of Joint Interagency Task Force South since 2004. In that capacity, he leads the Nation's premier international counter-narcotics efforts and coordinates the Department of Defense, Department of Homeland Security, Department of Justice efforts, along with numerous partners. Prior to that position, he was assigned as the Director of Operations Policy for the Coast Guard in 2003, responsible for managing a broad array of missions including Maritime Law Enforcement, Maritime Security and Defense Operations, Search and Rescue and National Boating Safety. In 2001 he was assigned as Director, Interagency Support and Anti Terrorism / Force Protection Division on the Navy Pentagon staff.

Admiral Hathaway added, "It has been my experience that one of the most challenging obstacles for law enforcement and border control is the ability to quickly and accurately identify people of interest in the field. It affects the speed with which we can apprehend criminals, the accuracy of arrests, and even the safety of officers as they perform their daily duties to the public. I am thrilled to have the opportunity to work with L-1, helping them to market their biometric solutions to government agencies tasked with solving these important issues."

Admiral Hathaway received the Defense Superior Service Medal, five Legion of Merit Awards, two Meritorious Service awards, two Coast Guard Commendation Medals and the 9/11 Medal.

Department of State Distinguished Honor Award Recipient Adds 30 Years of Experience in Identity Issues Related to International Travel

Frank Moss has more than 30 years experience working for the Department of State, as well as extensive experience working with other federal civilian, law enforcement and intelligence agencies. He received the highest performance award given by the Department of State (DoS), the Distinguished Honor Award, for leading the U.S. e-passport program and the Western Hemisphere Travel Initiative (WHTI). Most recently, Moss served as the Deputy Assistant Secretary for Passport Services for the DoS from

2003 to 2007. During his tenure, Moss expanded Passport Services to meet the doubling in demand and to improve turnaround time. Moss defended the design and security features of the U.S. electronic passport domestically and abroad before Congressional committees, privacy and travel groups, and private sector representatives. He also created the Passport Card to implement WHTI.

Prior to that, Moss served as the Executive Director of Bureau of Consular Affairs from 1998 - 2002, where he was responsible for the financial management, human resources, facilities management and information technology backbone necessary for the worldwide delivery of consular services. This included leading the effort to shift the Bureau to a fully fee-funded operation in the aftermath of 9/11 and the effects on U.S. Visa services. Under his leadership, the Bureau added hundreds of new overseas Foreign Service positions in the post 9/11 environment to make possible a radical realignment of consular work. Moss also managed the U.S. Border Crossing Card program.

"Producing a more secure and valid credential is at the heart of our ability to protect our citizens from crime, terrorism and fraud," said Moss. "For the past several decades, this is the issue that I have focused exclusively on solving for Americans. I am eager to apply this knowledge to L-1, helping advance the understanding of issues related to the passport and credentialing process in order to better market the innovative and important L-1 solutions to government agencies."

About L-1 Identity Solutions

L-1 Identity Solutions, Inc. (NYSE: ID), together with its portfolio of companies, offers a comprehensive set of products and solutions for protecting and securing personal identities and assets. Leveraging the industry's most advanced multi-modal biometric platform for finger, face and iris recognition, our solutions provide a circle of trust around all aspects of an identity and the credentials assigned to it -- including proofing, enrollment, issuance and usage. With the trust and confidence in individual identities provided by L-1 Identity Solutions, government entities, law enforcement and border management agencies, and commercial enterprises can better guard the public against global terrorism, crime and identity theft fostered by fraudulent identity. L-1 Identity Solutions is headquartered in Stamford, CT. For more information, visit www.L1ID.com.

SOURCE: L-1 Identity Solutions, Inc.

L-1 Identity Solutions

Doni Fordyce, 203-504-1109

dfordyce@L1ID.com

Copyright Business Wire 2007

News Provided by COMTEX

Board of Directors:

Robert V. LaPenta, Chairman of the Board, President and Chief Executive Officer

Robert V. LaPenta is Chairman of the Board, President and Chief Executive Officer of L-1 Identity Solutions. He has more than 30 years of executive management experience and has generated billions of dollars of shareholder wealth throughout his professional career. Mr. LaPenta founded L-1 Investment Partners in June 2005, leaving his position as president, CFO and board member of L-3 Communications to launch the company.

Mr. LaPenta co-founded L-3 Communications in 1997, following a successful 24-year executive career at Loral Corporation. He and his partners formed L-3 (which stands for Lanza, LaPenta and Lehman Brothers) as a leveraged buyout of ten advanced electronics business units from Lockheed Martin. Lockheed had merged with Loral Corporation in the prior year and Mr. LaPenta was CFO of Loral at the time of the merger. As president, CFO and board member of L-3, he guided the company to \$8 billion in annual revenue, EBITDA growth from \$60 million to \$1 billion and a stock-price appreciation from \$5 to \$170 pre-split. Mr. LaPenta also founded the Homeland Security Business, with annual revenues exceeding \$700 million.

During his seven-year tenure with L-3 Communications, the company completed more than 60 acquisitions, creating 60 individual business units run as separate entities under a common management approach that generated billions of dollars of shareholder wealth. While at Lockheed Martin and Loral Corporation, Mr. LaPenta served as corporate vice president and CFO of the C4ISR Group of Lockheed Martin from 1996 - 1997, where he led the Command, Control, Computer, Communication, Intelligence, Surveillance and Reconnaissance business sector with over \$8 billion in annual revenue. As corporate vice president for Loral Corporation from 1972 to 1996, he grew revenue from \$20 million to \$7 billion and EBITDA from a \$5 million loss to \$900 million.

B. Boykin Rose

B. Boykin Rose currently serves on the South Carolina Education Lottery Commission, to which he was appointed by Senator Glenn McConnell, President Pro Tempore of the Senate and Chairman of the Senate Judiciary Committee. He is an officer of Fear No Wind, LLC, a company he co-founded in 2004 and serves as Vice President of the Huguenot Society of South Carolina Board of Directors. Mr. Rose served as the Director of the South Carolina Department of Public Safety from 1993 to 2004. During his tenure as Director, Mr. Rose's responsibilities included establishment and administration of the Department's internal operation, policies and procedures and assumed direction of a number of departmental entities including the State Highway Patrol; the State Transport Police Division including the Size and Weight Enforcement Division; the Criminal Justice Academy and Training Division; the Highway Safety Office; the Division of Motor Vehicles which includes the Driver Licensing Division; Vehicle Registration; Vehicle Titling; Licensing and Vehicle Enforcement; the Bureau of Protective Services; and the Office of Justice Programs.

Admiral James M. Loy

Admiral James M. Loy joined the Viisage Board of Directors in 2006 and continued to serve through the company's merger with Identix that formed L-1 Identity Solutions. Admiral Loy brings extensive leadership experience and a deep understanding of national security to his position on the Board. He served as Deputy Secretary of the Department of Homeland Security from December 2003 to March 2005. Prior to this nomination by President Bush in October 2003, Admiral Loy was appointed by the Secretary of the U.S. Department of Transportation to become the Deputy Undersecretary for the then newly-formed Transportation Security Administration. Admiral Loy led the agency through its creation and subsequent incorporation into the Department of Homeland Security. Before entering public service, Admiral Loy served for 42 years in the U.S. Coast Guard, rising to the rank of Admiral and serving as the Commandant of the Coast Guard until 2002. He received many accommodations during his professional career, including the Distinguished Service Medal for the Department of Transportation, four Coast Guard Distinguished Service medals, a Defense Superior Service medal, and the Bronze Star with Combat "V," among others. He also received the NAACP Meritorious Service Award for 2000. In addition to the Viisage Board, Admiral Loy also currently serves on the Board of Directors for Lockheed Martin.

B.G. Beck, Vice Chairman of the Board

Mr. Beck is Vice Chairman of the Board for L-1 Identity Solutions. He was previously the Vice Chairman of the Board for Viisage and prior to that, he served as President and Chief Executive Officer of Trans Digital

Technologies Corporation from 1998 until its acquisition by Viisage in February 2004. Mr. Beck currently serves as a consultant to Viisage and also serves as a member of the Boards of Directors of Cardinal Bankshares Corporation, a provider of comprehensive individual and corporate banking services; and L-3 Communications MAS (US) Corporation, a leading supplier of a broad range of products used in a substantial number of aerospace and defense platforms.

Denis K. Berube

Mr. Berube previously served on the Board of Directors of Viisage since the company's incorporation in May 1996. During this time, he also served as Chairman of the Board from May 1996 to December 2005. Mr. Berube is Executive Vice President and Chief Operating Officer of Lau Technologies (referred to as Lau). Lau was one of the largest holders of Viisage Common Stock, directly owning approximately 7.5% of its issued and outstanding Common Stock. Mr. Berube has been employed at Lau since 1990.

George J. Tenet

George J. Tenet served as a member of the Board of Directors of Viisage from December 2005 until it merged with Identix to become L-1 Identity Solutions in 2006. Mr. Tenet formerly served a seven-year term as Director of Central Intelligence for the United States. Mr. Tenet's seven-year term as the Director of Central Intelligence was the second-longest in U.S. history. He first served as Deputy Director of Central Intelligence from 1995-1997 until he became the 18th Director of Central Intelligence in July 1997, following a unanimous confirmation vote in the United States Senate. As Director, Mr. Tenet led the U.S. Intelligence Community – a team of 14 foreign intelligence organizations – and presided over the daily activities of one of its members, the Central Intelligence Agency. He served as the Director until 2004.

Mr. Tenet received many awards for his public service. President George W. Bush awarded Tenet the Presidential Medal of Freedom in 2004, one of the two highest civilian awards in the U.S. The Presidential Medal of Freedom recognizes individuals who have made an especially meritorious contribution to the security or national interests of the United States, world peace, cultural, or other significant public or private endeavors. He also holds the two highest decorations for leadership from the Central Intelligence Agency and the United States Intelligence Community, receiving both the Distinguished Intelligence Medal and the National Intelligence Distinguished Service Medal. Mr. Tenet also has many foreign decorations and civic service recognitions.

Mr. Tenet came to the Intelligence Community from the National Security Council (NSC) where he was Special Assistant to the President and Senior Director for Intelligence Programs. In that office, he developed and coordinated policies on virtually every aspect of intelligence and espionage from collection priorities to covert action. Before joining NSC, Mr. Tenet was a member of President Clinton's national security transition team, responsible for a comprehensive assessment of the Intelligence Community. Prior to that, Mr. Tenet served in several Staff- and Staff Director-level positions within the Senate Select Committee on Intelligence (SSCI). He also served as Legislative Director for Senator H. John Heinz III.

Harriet Mouchly-Weiss

Ms. Mouchly-Weiss served as a director of Viisage from the time of its incorporation in May 1996 until the company merged with Identix and became L-1 Identity Solutions in 2006. She founded Strategy XXI Group, an international communications and consulting firm, in January 1993 and has served as its managing partner since that time. Ms. Mouchly-Weiss currently also serves as a member of the Board of Directors of American Greetings Corporation, a company engaged in the design, manufacture and sale of everyday and seasonal greeting cards and other social expression products.

John E. Lawler

John E. Lawler was a director of Identix from June 2002 until the company's merger with Viisage in 2006. He previously served on the Board of Directors of Visionics Corporation and Digital Biometrics, Inc. He also currently serves on the Board of Directors of NCI, Inc. Mr. Lawler has been President of East/West Financial Services, Inc., a diversified financial management and business consulting firm, since November 1987. He is also a co-founder of Sterling Wealth Management, Inc., a registered investment advisor and has served on its Board since October 1999. He currently serves as its Chief Executive Officer and Chairman of the Board. From November 1984 to March 1988, Mr. Lawler served as Executive Vice President of The Kamber Group, a public relations firm in Washington D.C. From March 1982 to October 1984, Mr. Lawler served as a Senior Vice President and Chief Financial Officer with Gray and Company, an advertising, public relations and lobbying firm. From January 1975 to March 1982, Mr. Lawler served as Chief of the Office of Finance of the U.S. House of Representatives in Washington, D.C.

Malcolm J. Gudis

Malcolm J. Gudis was a director of Identix from 2001 until the company's merger with Viisage in 2006. In 1993, he retired as a Senior Vice President of EDS where he had worked for 22 years. For six of those years, he served as a member of EDS' Board of Directors, and for eight of those years, he served on EDS' seven man Leadership Council. Mr. Gudis also had direct responsibility for EDS' international, commercial business interests outside of North America, including operations in over 30 countries as well as worldwide responsibility for the market segments comprising the Communications, Transportation and Energy and Petrochemical industries. In 1998, Mr. Gudis was awarded the first International Alumni Award by The Max M. Fisher School of Business at Ohio State University. He currently serves on The Dean's Advisory Council at The Fisher College of Business at Ohio State University, The Board of Trustees of The Episcopal School of Dallas where he serves as Chancellor, The Carnegie Council on Ethics & International Affairs and numerous charitable and business organizations.

Milton E. Cooper

Milton E. Cooper served previously on the Identix board from 2001 until its merger with Viisage in 2006. During that time, he was Chairman of the Board from 2004 - 2006. Mr. Cooper is the immediate past Chairperson for the Secretary of the Army's National Science Center Advisory Board. In 2002, he was recognized as the "20 Year Outstanding Industry Executive" by Government Computer News (a Washington Post Company). From 1992 until his retirement in June 2001, Cooper served as President, Federal Sector for Computer Sciences Corporation (CSC), one of the largest systems integrators for federal government agencies and a leading supplier of custom software for aerospace and defense applications.

Under his leadership, CSC's Federal Sector grew to more than 17,000 information technology professionals and accounted for approximately 25 percent of CSC's fiscal year 2001 annual revenues of \$10.5 billion. Cooper joined Systems Group, the predecessor organization to CSC's Federal Sector, in 1984, as Vice President, Program Development. Prior to joining CSC, Cooper served in various marketing and general management positions at IBM Corporation, Telex Corporation and Raytheon Company. Cooper has served on numerous committees and organizations including: Chairman, Armed Forces Communications and Electronics Association (AFCEA); Chairman, Secretary of the Army's National Science Center Advisory Board; Member of the board of directors of the Information Technology Association of America (ITAA); and National Defense Industrial Association and the USO.

Peter Nessen

Peter Nessen served as a director of Viisage from the time of its incorporation in May 1996 until the company merged with Identix and became L-1 Identity Solutions in 2006. Since July 2003, Mr. Nessen has served as the President of Nessen Associates Ltd., a non-profit consulting company. From January 2003 to July 2003, Mr. Nessen served as an advisor to the Governor of the Commonwealth of Massachusetts on education matters. Mr. Nessen has been Chairman of the Board of NCN Financial, a private banking firm, since January 1995. From June 1993 through December 1994, Mr. Nessen was Dean for Resources and Special Projects at Harvard Medical School.

Robert S. Gelbard

Mr. Gelbard formerly served on the Viisage Board of Directors and is Chairman of Washington Global Partners, LLC, a consulting company. He has had a distinguished diplomatic career as President Clinton's Special Representative for the Balkans from 1997-1999, Ambassador to Indonesia from 1999-2001, Ambassador to Bolivia from 1988-1991, and Assistant Secretary of State from 1993-1997. Further accomplishments include serving as the U.S. Government's representative to the Paris Club and as President George H.W. Bush's personal representative to the 1992 San Antonio Summit. Ambassador Gelbard has devoted his expertise in economics, law and diplomacy to developing and implementing numerous post-conflict strategies in Central Europe, Latin America and the Caribbean, Africa and Southeast Asia, supporting South America's efforts to return to democratic governance and initiate market-oriented economic policies, U.S. policy to support democratic consolidation in Spain and Portugal, and U.S. policy towards Southern Africa to affect fundamental societal change. In 2002, Ambassador Gelbard received the Distinguished Service Award, the State Department's highest commendation, which was conferred by Secretary of State Colin Powell. Ambassador Gelbard is also the recipient of numerous other commendations from the U.S. and foreign governments.

MANAGEMENT TEAM:

Bruce Hanson, President, SecuriMetrics, Inc./Iridian Technologies

Bruce Hanson is President of SecuriMetrics, Inc./Iridian Technologies. Mr. Hanson has over 24 years of experience in business development and management within various technology fields. Mr. Hanson joined SecuriMetrics in 2005 and has served in several capacities including SVP Sales & Marketing, COO and presently President.

Prior to joining SecuriMetrics, Inc., Mr. Hanson was President and CEO of Streampipe Corporation, which provided rich media software and services to corporations and federal government clients. During his tenure at Streampipe, Mr. Hanson successfully led the company through multiple financings as well as several acquisitions and ultimately the merger of the company with Loudeye Corporation (NASDAQ: LOUD).

Prior to leading Streampipe, Mr. Hanson was the President and CEO of TEN-TV Corporation, the acquirer of Streampipe. TEN-TV provided clients with ASP based solutions for on-demand corporate communications and field training using the internet. In 1992, Mr. Hanson served as President & CEO of New York based STV Corporation (Satellite Television Corporation). STV provided high-tech companies with outsourced global video communications capabilities using leased satellite transponders.

Prior to STV Corporation, Mr. Hanson co-founded Westcon Group and served as its Senior Vice President of Marketing where he managed the worldwide Westcon brand and established marketing and sales communications programs across multiple geographies and technology platforms. Mr. Hanson's contributions help propel the company from one office and sales of \$6 million to 23 offices in 14 countries and sales in excess of \$1.2 billion. Westcon Group was subsequently sold to South African distributor, Data Tech Corporation. Mr. Hanson began his career with IBM Corporation in the National Distribution Division.

Charlie Carroll, CEO of IBT, Inc.

As CEO of IBT, Charlie Carroll is responsible for the Company's overall management, development, and growth. Currently, he is active in implementing IBT's strategic plan and overseeing major initiatives. Mr. Carroll is also the President and CEO of ASET Corporation, an investigative and security consulting firm.

He is nationally recognized as an authority on drug abuse, drug trafficking, violence prevention, and the "principals of protection." Mr. Carroll is an expert in the development of procedures used to conduct undercover operations in corporate facilities and government agencies, as well as, vulnerability and threat assessments. Since 1988, he has trained over a quarter million managers, supervisors, and employees to spot the signs and symptoms of the drug-affected person and how to prevent violence in the workplace. His procedures and techniques, designed for supervisory coaching and intervention programs, are being used throughout the United States in many Employee Assistance Programs.

Previously, Mr. Carroll was Vice President of Business Risk International (BRI), the Professional Law Enforcement (PLE) Division. He co-founded PLE, Inc. in 1981 and developed PLE Testing Laboratories, a forensic drug and urine-screening laboratory. Mr. Carroll majored in Criminal Justice Studies in college. He was formerly an officer with the Dayton, Ohio, Police Department, where he specialized in narcotics, organized crime, and motorcycle gang enforcement. He managed and participated in long-term undercover operations. Since then, he has been responsible for the management and performance of over 5,000 undercover drug investigations resulting in over 35,000 arrests. In addition, he is an active member of the American Society of Industrial Security (ASIS) and the National Drug Enforcement Officers Association (NDEOA).

Doni Fordyce, Executive Vice President, Corporate Communications

Doni Fordyce is Executive Vice President of Corporate Communications for L-1 Identity Solutions and serves as a partner of L-1 Investment Partners. She brings two decades of senior executive and investment management experience to the company, serving most recently as CEO, president and COO of Bear Stearns Asset Management (BSAM) Inc. Under her leadership, the firm's assets grew at a 25 percent CAGR from \$6 billion to \$24 billion. Prior to that, Ms. Fordyce was vice president of Goldman Sachs Inc. from 1986 to 1996 where she was one of the founders of the asset management business. She has also worked in IT solutions consulting, specializing in networking, data management and printing for investment banks and financial institutions.

Dr. Joseph Atick, Executive Vice President, Chief Strategic Officer

Dr. Joseph Atick is Executive Vice President and Chief Strategic Officer of L-1 Identity Solutions, where he sets overall strategic direction for product development, technology investment and support of merger and acquisition activities. Dr. Atick is known as one of the early pioneers of the biometrics industry, having seen through its early phases through the validation and commercialization growth phase we are witnessing now. Prior to joining L-1 Identity Solutions, Dr. Atick served as President and CEO of Identix, today an L-1 Identity Solutions Company. Prior to that, he had co-founded one of the original facial recognition companies, Visionics Corporation.

Over the years, Dr. Atick co-founded and managed several companies focused on technology transfer and development, and has served as a technical advisor to many high-tech enterprises and organizations, including NATO. He had also led the Computational Neuroscience Laboratory at Rockefeller University and the Neural Cybernetics Group at the Institute for Advanced Study in Princeton, New Jersey. Dr. Atick is a highly sought after speaker at high level industry conferences and a frequent commentator in the media. He has also been asked to testify several times before congressional committees. Dr. Atick holds a Ph.D. in Mathematical Physics from Stanford University.

James DePalma, Executive Vice President, Chief Financial Officer and Treasurer

Jim DePalma is Executive Vice President, Chief Financial Officer and Treasurer of L-1 Identity Solutions and serves as a partner of L-1 Investment Partners. He brings three decades of operational and finance experience in the defense and technology industries to his role within the company. Prior to the formation of L-1 Investment Partners, Mr. DePalma served as a consultant to L-3 Communications and was the chief executive officer of Core Software Technology, a leading software provider to the intelligence community and an L-3 equity investment.

Jim Moar, President of Identix, Inc.

James Moar is President of Identix, Inc., an L-1 Identity Solutions company. He has more than 23 years of operational management expertise. He most recently served as Chief Operating Officer for Identix. Prior to his position at Identix, Mr. Moar served a combined twelve years as Chief Operating Officer of both DataCard Group and the Tennant Company.

Joseph Paresi, Executive Vice President, Chief Marketing Officer

Joe Paresi is Executive Vice President and Chief Marketing Officer of L-1 Identity Solutions and is a partner of L-1 Investment Partners. Mr. Paresi brings three decades of executive management, product development, and design engineering experience in the technology and defense industries to his role within the firm. Prior to joining L-1 Investment Partners, he served as corporate vice president of product development for L-3 Communications and as president of L-3 Security & Detection Systems from 1997 to 2005.

Mark S. Molina, Executive Vice President, Chief Legal Officer and Secretary

Mark S. Molina is Executive Vice President, Chief Legal Officer and Secretary of L-1 Identity Solutions. He is a business and technology lawyer with over 20 years of top-tier legal experience structuring and negotiating mergers, acquisitions, dispositions, joint ventures, technology licenses, financings and investments. He has considerable experience with public offerings and private placements, as well as the SEC reporting and compliance obligations of publicly traded companies. Prior to joining L-1 Identity Solutions, Mr. Molina was the Executive Vice President, Chief Legal Officer and Secretary for Identix.

Vincent D'Angelo, Senior Vice President, Finance and Chief Accounting Officer

Vincent A. D'Angelo is Senior Vice President of Finance for L-1 Identity Solutions and serves as a member of the senior team at L-1 Investment Partners. He brings extensive experience in accounting and auditing, operations, business systems, risk management, international, and mergers and acquisitions. Prior to joining L-1 Investment Partners, Mr. D'Angelo was a senior audit partner with PricewaterhouseCoopers for more than 35 years where he was involved in all facets of the business, including client service, management, operations, governance, SEC filings, and technical leadership. He also served an integral role in the development of PwC's M&A practice, developing many of the techniques, methodologies and approaches used by the firm and performing hundreds of M&A transactions.

Viisage Awarded Over \$48 Million in Contracts to Help States Meet Requirements of the REAL ID Act

[source: <http://ir.l1id.com/releasedetail.cfm?ReleaseID=207972>]

BILLERICA, Mass., Jun 13, 2006 (BUSINESS WIRE) -- Viisage (Nasdaq: VISG), a leading provider of advanced technology identity solutions, today announced that the Departments of Transportation/Motor Vehicles in Pennsylvania, Wisconsin, Maryland and Arkansas have awarded new contracts or extensions to the company for innovative solutions to help provide security in the states' driver's licensing processes and procedures required of the federal REAL ID Act. The contract awards total more than \$48 million and vary in length from six months to over seven years.

The contracts recently awarded to Viisage include key wins from major US states:

-- The Pennsylvania Department of Transportation (PennDOT) awarded Viisage \$45.5 million in contracts. The contracts augment and strengthen the existing technology and solution to further secure the drivers' licensing process.(a)

-- The Wisconsin Department of Transportation awarded Viisage a \$500,000 contract to implement automated document authentication to vet claimed identities prior to issuing valid driver's licenses. Wisconsin has been a customer since 1997 and in 2005 awarded the company a \$7.5 million contract for issuance of driver's licenses and ID cards.

-- The Arkansas Department of Finance and Administration awarded Viisage a \$2 million contract extension to continue the state's secure driver's licensing program. This extension follows the 1999 contract award and subsequent extensions which totaled \$15 million.

-- The Maryland Department of Motor Vehicles awarded Viisage a \$300,000 services extension on the contract Viisage won in 1999 for a secure driver's license solution. Awards and extensions from Maryland to date total over \$9 million.

"We look forward to our ongoing partnership with Viisage as we move ahead with continued improvements to ensure the security of PennDOT's driver licensing products," said Betty Serian, Deputy Secretary for Safety Administration, PennDOT.

"These significant wins exemplify our leadership position in the marketplace, as we provide a myriad of solutions to help the states combat identity theft and fraud and comply with the REAL ID Act," said Bernard Bailey, president and CEO of Viisage.

Driver's licenses and IDs produced by the states in the U.S. continue to be important identity documents in personal transactions such as banking and travel. In May 2005, the Real ID Act was passed, challenging states to increase security in select identity documents and provide a means

for interstate verification of an applicant's identity. Viisage provides a variety of end-to-end identity products, services and solutions to the driver's license marketplace for these initiatives, including the following: designing and developing secure driver's license and ID solutions; examining and verifying an identity prior to issuing a secure credential; automating document authentication for identity verification; detecting individuals suspected of identity theft or fraud; providing biometrics such as face recognition and fingerprint technologies for uniquely tying individuals to their identity documents and for investigation; and reconciling duplicate database records.

(a) Includes the seven-year extension previously announced on Viisage's quarterly earnings call on May 15, 2006

About Viisage

Viisage (NASDAQ: VISG) delivers advanced technology identity solutions for governments, law enforcement agencies and businesses concerned with enhancing security, reducing identity theft, and protecting personal privacy. Viisage solutions include secure credentials such as passports and drivers' licenses, biometric technologies for uniquely linking individuals to those credentials, and credential authentication technologies to ensure the documents are valid before individuals are allowed to cross borders, gain access to finances, or be granted other privileges. With more than 3,000 installations worldwide, Viisage's identity solutions stand out as a result of the company's industry-leading technology and unique understanding of customer needs. Viisage's product suite includes IdentityTOOLS™ SDK, Viisage PROOF™, FaceEXPLORER®, iA-thenticate®, ID-GUARD®, BorderGuard®, PIER™, HIIDE™, AutoTest™, FacePASS™ and FaceFINDER®.

This news release contains forward-looking statements that involve risks and uncertainties. Forward-looking statements in this document and those made from time to time by Viisage through its senior management are made pursuant to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. These forward-looking statements reflect the Company's current views with respect to the future events or financial performance discussed in this release, based on management's beliefs and assumptions and information currently available. When used, the words "believe", "anticipate", "estimate", "project", "should", "expect", "plan", "assume" and similar expressions that do not relate solely to historical matters identify forward-looking statements. Forward-looking statements concerning future plans or results are necessarily only estimates and actual results could differ materially from expectations. Certain factors that could cause or contribute to such differences include, among other things the size and timing of contract awards, performance on contracts, performance of acquired companies, availability and cost of key components, unanticipated results from audits of the financial results of the Company and acquired companies, changing interpretations of generally accepted accounting principles, outcomes of government reviews, developments with respect to litigation to which we are a party, potential fluctuations in quarterly results, dependence on large contracts and a limited number of customers, lengthy sales and implementation cycles, market acceptance of new or enhanced products and services, proprietary technology and changing competitive conditions, system performance, management of growth, dependence on key personnel, ability to obtain project financing, general economic and political conditions and other factors affecting spending by customers, and the unpredictable nature of working with government agencies. In addition, such risks and uncertainties include, among others, the following risks: that the merger with Identix will not close, that the regulatory or shareholder approval will not be obtained, that the closing will be delayed, that customers and partners will not react favorably to the merger, integration risks, the risk that the combined companies may be unable to achieve cost-cutting synergies, and

other risks described in Viisage's and Identix' Securities and Exchange Commission filings, including the Registration Statement on Form S-4 filed with the SEC in connection with the transaction, Viisage's Annual Report on Form 10-K for the year ended December 31, 2005 and its Quarterly Report on Form 10-Q for the quarter ended March 31, 2006 under the captions "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations," and Identix' Annual Report on Form 10-K for the year ended June 30, 2005 and its Quarterly Reports on Form 10-Q for the quarters ended September 30, 2005, December 31, 2005 and March 31, 2006 under the captions "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations." Viisage expressly disclaims any obligation to update any forward-looking statements.

SOURCE: Viisage

L-1 Investment Partners
Doni Fordyce, 203-504-1109
dfordyce@L-1ip.com
or
Viisage
Chad Crouch, 703-414-5474
ccrouch@Viisage.com

Friday, January 27, 2006

L3 founder LaPenta to put a new face on Viisage

http://boston.bizjournals.com/boston/stories/2006/01/30/newscolumn3.html?jst=pn_pn_lk

Boston Business Journal - by Alexander Soule Journal Staff

It has never been easy to capture the face behind **Viisage Technology Inc.**, but let's take one last look before the company gets merged into a Minnesota counterpart.

There is no question today whose fingerprints are all over the facial recognition software company in Billerica, and it's no mystery what Bob LaPenta is eyeballing now.

Last fall, Viisage decisions shifted from the company's Billerica headquarters to Stamford, Conn., thanks to the \$100 million La-

Penta implanted into Viisage via his L-1 Investment Partners LLC fund in Stamford.

LaPenta's latest rollup involves Viisage and **Identix Inc.**, the Minnesota fingerprint scanner manufacturer, intending to create a mini **L-3 Communications Holding Corp.** in biometric security.

LaPenta is credited as being one of the three L's in L-3, the security conglomerate created from technologies spun out of the 1997 merger between Maryland's **Lockheed Martin Corp.** and the former Loral Corp.

Viisage and Identix have yet to choose a name for when the merger closes. May I suggest L-2 Technology?

The first "L" would refer to LaPenta. The second "L" would pay tribute to Viisage visionary Joanna Lau, who ranks among Massachusetts' most intriguing and successful female technology entrepreneurs, right up there with **iRobot Corp.** co-founder Helen Greiner.

In 1990, Lau and spouse Denis Berube, technicians who met at General Electric Co., engineered the buyout of **Bowmar Acton Laboratories** just as Lau wrapped up her MBA from **Boston University**.

According to one account, they put together the deal on \$400,000 from savings and a second mortgage, a \$1.2 million bank loan, \$750,000 in a Small Business Administration loan guarantee, \$450,000 from 25 Bowmar employees and a \$300,000 loan from Bowmar's former owners.

Renamed Lau Technologies, the lab continued to produce fire-control systems for U.S. Army armored combat vehicles. At the same time, it spun out Viisage as an independent company in 1993.

The early Viisage sold processing stations equipped with cameras, lights, computers, bar code readers, signature-capture screens -- everything needed to produce tamper-proof driver's licenses.

Opposing Sides Work Together to Derail Real ID

It's not just Conservative-driven grass roots organizations such as Gun Owners of America and members of the "Christian Coalition" that continue to raise objections to final implementation of the REAL ID Act of 2005.

A far-reaching and ever-growing coalition made up of hundreds of traditionally clashing organizations from the American Bar Association and the American Civil Liberties Union to the Competitive Enterprise Institute and the National Taxpayers Union are now standing together in opposition due to the following Constitutional and economic concerns:

1. REAL ID is likely to conflict with any type of privacy, free speech, religious or other fundamental personal liberty protections guaranteed in each state's constitution.
2. REAL ID could overrule any state controls over what type of information can be included or excluded from state driver's licenses.
3. With a standardized national machine-readable zone, REAL ID will make it even easier for police officers and retail clerks—as well as unscrupulous credit card companies and telemarketers—to access your most personal information.
4. REAL ID offers absolutely no controls on what confidential data can be collected from driver's licenses, where and how long it can be stored and who is authorized or unauthorized to obtain, share, trade or sell that information.
5. Moving well beyond the national driver's license registry, REAL ID is a key lynch-pin in the U.S. government's Security and Prosperity Partnership agreement between Mexico and Canada—a non-legislative effort to form a North American version of the European Union.

6. Not only would REAL ID jeopardize the privacy of every American citizen on a national scale, but it could easily establish an agreement with Canada and Mexico to provide equal and non-supervised access to your most confidential information as well.
7. From an economic standpoint, such diverse groups as the National Governor's Association, National Conference of State Legislatures and the American Association of Motor Vehicles are predicting that REAL ID will cost state governments no less than **\$11 billion** to implement this completely unfunded federal mandate.
8. According to the latest collaborative survey conducted across 47 states by the groups listed above, there are also hundreds of millions of dollars in unforeseen costs such as the added time and effort citizens must spend in order to comply with their respective state's motor vehicle department.
9. With an average of three to four identity documents per applicant and 80 million transactions performed annually, applicant processing time will more than double for citizens in most states—with waits in some areas increasing up to **200 percent**.
10. Several provisions under consideration by the Department of Homeland Security could also dramatically add to the increased taxpayer costs described above.

The REAL ID Act is an unwarranted, fiscally irresponsible, big government rejection of states' rights and state sovereignty that must not go unchallenged.

Extract from "Rohrer Sounds Warning Against REAL ID Act"
A flyer published by Rep. Sam Rohrer, District 128, Penna. House of Representatives,
and the Republican Caucus of Pennsylvania

REAL ID-BIOMETRIC FACT SHEET

The Final Chapter in a Systematic Plan for Global Biometric ID

Submitted by STOP REAL ID – an association of concerned citizens

The REAL ID ACT of 2005 is not a national ID card but an INTERnational BIOMETRIC ID card

The world is being enrolled in an international biometric ID system through driver's license/ID cards (DL/ID cards), passports and other ID documents. The federal government attempted to impose biometrics on state ID in 1986ⁱ. International biometric plans were laid in 1995ⁱⁱ. Both predate 9/11. The biometrics required by REAL ID, other security laws, initiatives, treaties and agreements, are not needed tools against terrorism, but the fulfillment of a global biometric ID system.

On March 1st, 2007 REAL ID's "Notice of Proposed Rulemaking" (NPRM) was issued, revealing REAL ID's global biometric connectionⁱⁱⁱ. The three main entities driving this system are:

1. The Department of Homeland Security (DHS)
2. The American Association of Motor Vehicle Administrators (AAMVA)
3. The International Civil Aviation Organization (ICAO)

AAMVA is an international association of motor vehicle and law enforcement officials^{iv}. AAMVA is responsible for international biometric DL/ID card standards and a (DMV-DPS) data linking system, the "Driver License Agreement" (DLA)^v. The most recent AAMVA DL/ID standard is the 2005 "Personal Identification – AAMVA International Specification- DL/ID Card Design."^{vi} The 2005 DL/ID standard, DLA and various other document standards are requirements, cited in REAL ID^{vii} and NPRM^{viii}. AAMVA exercises great influence over international, federal and state level DL/ID card laws, evident in REAL ID (AAMVA is mentioned 30 times in NPRM).



ICAO monitors travelers, designed biometric "e-passports"^{ix} required for "Visa Waiver Nations"^x and is affiliated with the UN^{xi}. Global enrollment into the e-passport system is 50 million annually^{xii}. REAL ID photos comply with ICAO "**biometric data interchange formats**"^{xiii} standards, making state photos compatible with global biometric facial recognition standards.

Together, DHS, AAMVA and ICAO are fulfilling the three elements necessary for a global biometric system.

1. Common "interoperable" document and biometric standards set by ICAO-AAMVA
2. Biometric enrollment (passports, DL/ID cards, military ID, government employee ID, birth records, etc.)
3. International database linking containing personal-biometric information (DHS-AAMA-ICAO)

REAL ID and NPRM require states to:

1. Adopt biometric photo standards set in ICAO 9303^{xiv}, a minimum resolution of 90 pixels between eye centers
2. To verify identification "breeder" documents and supporting documents through an online system (proposed systems include DHS sponsored "federated querying"^{xv} and AAMVAnet^{xvi})
3. Adopt documentation standards set by AAMVA
4. Link state databases and participate in AAMVA's DLA

After issuing the NPRM, DHS released "20 Questions and Answers"^{xvii} about REAL ID. In it, DHS

denied:

Creating a national ID card

Creating a national database on applicants

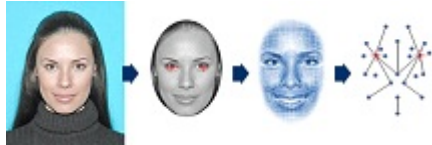
Requiring biometrics for state ID or storing biometric information from state ID

REAL ID is an INTERnational ID. DHS can “legally” access database information through the outdated “Drivers Privacy Protection Act” (DPPA) and the DHS proposed “federated querying system.” REAL ID DOES require photos compatible with facial recognition biometrics and any government agency accessing the linked database system can use any state photo with facial recognition software, making it a biometric.

REAL ID standards make state databases “interoperable” and database linking will result in states losing control of their ID system. The DL/ID card controls our ability to buy, sell and move. While under state control, this power remains under the control of the people who have access to the lawmakers administering its use. REAL ID places that control under federal and international entities through laws, initiatives and treaties, some of which are listed below.

FACIAL RECOGNITION – The Global Biometric of Choice

Facial recognition creates a digital, machine readable, map of one’s face. 3-D facial recognition potentially identifies individuals in “real world” settings, addressing issues of lighting and movement, providing the tool for a surveillance society like Great Britain with an estimated 500,000 surveillance cameras in London and 7 million nationally.^{xviii}



On June 28, 2002, the ICAO, and its stakeholders, unanimously endorsed the “*Berlin Resolution*” for “*the use of facial recognition as the globally interoperable biometric for machine assisted identity confirmation with MRTD’s (machine readable travel documents)*”^{xix} **Why Facial Recognition? Facial recognition can use existing digital photo databases (enrollment) and is suitable for public surveillance.**

FACIAL RECOGNITION TESTS –

National security funds are wasted on biometrics. Facial recognition failures are highly documented^x even in AAMVA’s 2003 “International Biometric Group” (IBG) report^{xxi}. The report “anticipates” (by two years), the linked database requirements of REAL ID (300 million drivers), demonstrating AAMVA’s influence on federal legislation.

The IBG report reveals:

“Synopsis of facial image recognition performance is **POOR.**”

Test results on a “**100-person database**” showed “**only “53% of multiple enrollees were identified correctly”** and “*The comparatively small size of this database, and the error rates encountered, call into question the scalability of facial recognition for much larger systems*”(pg 10).

“...facial recognition will **not be capable** of successfully performing 1:300m (million) identification”(pg 17).

IBG evaluated a Colorado DMV case study using facial recognition to look for duplicate DL/ID cardholders. On 3000 applicants/day, the facial recognition program produced 100-125 facial image matches/day. “**False Matches**” were 99% of those, making **only 1% valid** (about 1 per day or 26 per month (pages 93-94).

Facial recognition has great difficulty with facial hair and glasses (pages 30-32, 117).

“**Vendor’s performance projections**” - “**Estimated 69% correct ID rate on 300m (million) database**” (pg 16). Vendor claims for a 1:300 million environment, exceed the small 100-person database test result (53%)!

The DHS sponsored, Facial Recognition Vendor Test 2006 (FRVT 2006)^{xxii} also reflected inflated vendor estimates, prompting biometrics expert, Ben Bavarian to state that the tests are “*only valid for the defined circumstances of the NIST ITL labs*” and these tests are “*turned into marketing tools for vendors to push the products without doing the right things for the technology.*”

DHS WANTS MORE HIGH-TECH TOOLS—Human Dignity, Civil Rights, Testing & Function are Secondary



Like facial recognition, DHS shares equal disregard for other testing procedures. On September 18, 2007, the Washington Post reported,^{xxiii} that weeks before key government tests of new radiation detection equipment, DHS officials “helped” contractors through repeated dry runs that enabled them to perform better during the examinations. Congress expected to use the long-awaited tests to make a \$1.2 billion decision. Congress was previously concerned that DHS misled them about the device’s effectiveness, known as Advanced Spectroscopic Portals, or ASPs.

Instead of investing in “real” security, DHS spent millions on Boeing’s “virtual fence,” that doesn’t work.^{xxiv} DHS is also testing the “virtual strip search,” machine, AKA-backscatter device, recently deployed in Phoenix.^{xxv} Another new item being tested is “Project Hostile Intent”^{xxvi} that will “*identify*” terrorists’ “*intent*” by judging behavior and facial expressions. The suspect test procedures and failed tests by DHS-TSA are too numerous to mention in this document.

POWER, CONTROL AND DECEIT

Consider the numerous technology failures, the deceit of government agencies and the constitutional risks. How can we trust biometrics, biometric vendors, international organizations and government agencies employing biometrics? REAL ID grants DHS almost unlimited powers. DHS can also redefine their powers as they see fit. NPRM states that the “official purpose” of REAL ID: “*includes but is not limited to accessing Federal facilities, boarding Federally-regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine.*” The section goes on to say, “*...under the discretionary authority granted to the Secretary of Homeland Security under the Act, may expand this definition in the future.*”

REAL ID’s official purposes have already changed to discourage further opposition i.e. access to national parks. Potentially, REAL ID requirements could be imposed on banking, Medicare or cashing Social Security checks, school ID, etc. **REAL ID is a symptom of a society that has lost control of its government, where international organizations have more influence over state and federal law than the people, or their elected representatives.**

DL/ID Card Photo = Biometrics and deceitful enrollment. Why use facial recognition? Enrollment. The 2003 IBG report states, “*Facial recognition technology can acquire faces from almost any static camera or video,*” and “*Facial recognition databases...are capable of creating databases from facial images not specifically collected for biometric usage.*” Linked databases with photos = facial recognition database.

RUSHING TO FAILURE – Increasing Risk and Wasting Resources

Robert Moczny (DHS US-Visit) stated that “*information sharing is appropriate around the world,* and DHS plans to create a “*Global Security Envelope of internationally shared biometric data that would*

permanently link individuals with biometric ID, personal information held by governments and corporations.”^{xxvii} DHS is committed to global data sharing and is “rushing” to fulfill a global biometric dream, before November 2008. Risking it all, DHS ignores the facts about, global biometrics, data sharing, allowing international organizations to influence U.S. law and REAL ID.

Global biometric ID and database linking threaten religious rights, privacy, states’ rights, and our sovereignty.

Database linking-sharing will certainly result in an ID theft pandemic. The consolidation of power in one document increases the chances of ID fraud just as data sharing increases the risk of ID theft.

Facial recognition will NOT work effectively on terrorists unless they submit to enrollment and *shave*.

Other countries will issue biometric ID based on their own “breeder” documents (ex. birth certificate). Based on those “breeder” documents, e-passports will be accepted at face value. Persons issuing, those documents, must be experts in identifying fraudulent “breeder” documents or the biometric ID permanently legitimizes the fraud.

This system places our national security on the shoulders of government employees in Peru, Columbia, Haiti, Bolivia, Pakistan, Saudi Arabia, China, etc.

Every government must have secure “records” buildings, information technology systems and totally trustworthy employees protecting highly personal information collected globally (shared databases). DHS-TSA lost a hard drive with thousands and thousands of employee records. How will they secure ID systems of other nations?

DHS has difficulties with information sharing between all levels of law enforcement. How can we rely on other nations to share accurate and highly personal information on all their citizens?

REAL ID, Western Hemisphere Travel Initiative (WHTI), e-passport, Transportation Worker Identification Credential (TWIC), backscatter, virtual fence, “Project Hostile Intent” etc. are indicators of the current DHS mindset that can’t keep its hands out of the technological cookie jar. While technical failures mount, our nation becomes less secure. DHS is wasting billions of dollars on “high-tech” failures instead of investing in fences and people desperately needed on our borders and in our ports. This “DHS mindset” has not escaped the notice of the Government Accounting Office (GAO), that recently cited many problems with DHS, giving it a several failing grades.

REAL ID and other biometric laws must be repealed. States must take back power from international organizations, wipe databases of biometrics and biometric compatible information, and reduce the quality of photos, making them unusable for biometrics (max. 25 pixels between eye centers), protecting state databases from future takeovers.

A CHRISTIAN PERSPECTIVE on REAL ID and BIOMETRICS

This document is an attachment to "REAL ID-BIOMETRIC FACT SHEET"

Submitted by STOP REAL ID – an association of concerned citizens

THE THREAT

The REAL ID ACT of 2005 has provoked opposition from all aspects of our society. New Hampshire's ban of REAL ID called it "repugnant." Many conservative Christians oppose REAL ID for religious reasons. Other groups, like the ACLU, oppose REAL ID but for reasons of privacy. Opposition to REAL ID is more like a war, where differences are thrust aside because of a common enemy. For example, REAL ID requires digital photographs (compatible with biometric facial recognition). Therefore it violates the religious beliefs of some smaller Christian denominations, like Mennonites, but it also violates the religious rights of many Muslim women. The issue is protecting freedom for all. This concept was not wasted on Corrie ten Boom or Dietrich Bonhoeffer, the great German theologian of WWII, who died preserving such freedoms.

REAL ID also threatens the beliefs of mainstream, conservative, evangelical Christians. Biometrics and database linking create an international system of financial control linked to one's body similar to the mark of the beast described in the Book of Revelation. Biometrics is an international ID system with standards, set by international organizations. The purpose of these standards is to create a platform for sharing personal-biometric data globally. Global data sharing is not possible unless nations and states link databases (required by REAL ID). The Department of Homeland Security (DHS) has made it very clear that personal-biometric information, collected by nations and corporations, will be shared globally. Similar to Revelation 13:16, this global ID system would apply to "all" just like the mark of the beast.

Rev 13:16-17 (NAS)

16 And he causes all, the small and the great, and the rich and the poor, and the free men and the slaves, to be given a mark on their right hand, or on their forehead,
17 and he provides that no one should be able to buy or to sell, except the one who has the mark, either the name of the beast or the number of his name.

Biometrics and global data sharing create a system of financial control linked to one's body similar to Revelation 13:16-17. This is accomplished in two main ways.

1. Allowing and preventing financial transactions based on biometric enrollment and possession of biometric ID

The current "official purposes" of REAL ID would prevent the use of a non-compliant driver's license/ID card (DL/ID card) for flying commercially, entering federal buildings or entering nuclear power plants. More recently, DHS added national parks to that list. However, DHS powers are not limited to those purposes. REAL ID requirements can apply for "*any other purposes that the Secretary shall determine.*" and that DHS "*may expand this definition in the future.*" Potentially, only a REAL ID - DL/ID card could be used for banking, cashing Social Security checks, Medicare, etc. Before the 2007 "Immigration Bill" was stopped, biometric Social Security cards were proposed, and employment would be contingent upon possession of a REAL ID card. In other words, the trend is NO BIOMETRICS = NO buying, selling and driving or flying. Of course, one could use a passport for official federal purposes, but they are biometric now as well.

2. Using biometrics for identification in the completion of a financial transaction

In 1996, AAMVA proposed a universal biometric DL/ID Smart Card, replacing ALL other ID and financial documents. A microchip would store biometric and personal information (much like the new e-passport today). ID would be verified before by a hand or facial scan. More recently VISA-USA began testing a "fingerprint" credit system (no plastic). Since 1996, there have been, literally thousands of financial uses for biometrics.

IS THIS THE ENROLLMENT FOR THE MARK OF THE BEAST?

The current biometric ID system is not the mark of the beast, but would easily qualify as the enrollment process for it. Imagine, a linked database system, containing the personal and biometric information of almost every person in the world, accessible from almost anywhere in the world. This is the disturbing "vision" of DHS and, unfortunately, it is happening at a staggering rate. The ICAO estimates global enrollment into the biometric e-passport system to be 50 million annually.

THE MARK?

For years many have speculated that the mark may be a microchip. Recently a company called Somark (St. Louis, MO) developed ink RFID "tattoos" that works like a standard RFID chip. RFID chips store and transmit information just like a "Turnpike Pass". A signal is transmitted that activates the RFID chip. The chip then transmits its stored information. ID information is stored in the "digital ink" RFID "mark" or "tattoo" imbedded in the skin and is currently being targeted for cattle, industrial and military applications. Technologies like the RFID tattoo may provide clues as to what the "mark" of Revelation 13 might be.

PERMANENT ENROLLMENT

Biometric enrollment could occur simply through database linking (required by REAL ID). Existing digital photos, in DL/ID databases, could be used for biometric facial image recognition. Linked with other personal information, data could be shared globally even without one's knowledge. This is why ICAO and DHS elected to use facial image recognition as the biometric of choice for global data sharing. Also, facial recognition is suitable for public surveillance, identification and tracking.

DHS engaged in wishful thinking when deploying facial recognition biometrics. The tests available at the time current laws and initiatives were written, proved the ineffectiveness of facial recognition. Yet, DHS pushed this technology on U.S. citizens, spending millions and millions on an almost worthless tool against terrorists. Biometrics is about control, not security.

Try to get your Social Security number out of the "credit reporting" system. Impossible? It is impossible because of database sharing. REAL ID and systems used by DHS, would link the databases of states and nations. Linked databases would PERMANENTLY enroll Christians in a system, similar to one of Revelation 13. A system God will condemn. What greater threat to religious freedom is there than this?

SPECULATING ABOUT THE FUTURE

We may speculate over what kind of event would prompt the world to adopt the "mark?" ID theft? The potential of ID theft, in such an enormous global system, is mind-boggling. For such risks to be ignored by DHS and Congress defies explanation. But, a global ID theft pandemic COULD, prompt the introduction of "*other technological solutions*" where one is identified from birth using a mark. *Even under REAL ID, DHS will have the power to restrict buying, selling and moving, unless the individual has a biometric ID. Once databases are linked, we cannot get out, solidifying that control and power over our lives.* It is therefore, conceivable how, a world in a financial disaster, might embrace "other technologies."

HOW WILL CHRISTIANS ESCAPE THIS SYSTEM, WHILE THE WORLD IS ENROLLED?

U.S. citizens can stop REAL ID, biometrics and database linking in the U.S. We can also influence other nations to accept our non-biometric passports (even after we compelled other nations to adopt biometrics). If this system is the enrollment process for the “mark” then it is likely that it cannot be stopped globally. ICAO, and UN, influence is significant. ICAO began work on the biometric e-passport in 1995, long before 9/11. However, as Christians, we believe God will provide a way of escape that we may be able to endure (1 Cor 10:13).

In the United States we have constitutional rights protecting our religious freedom. It is therefore probable that the United States will become a safe haven, protecting Christians from enrollment while the rest of the world is enrolled. The irony, of course, is that we imposed this system on the world.

HOW CAN THIS SYSTEM BE STOPPED?

By February 2008, states must decide to defy REAL ID or participate in it, and request an extension. REAL ID goes into effect May 11th, 2008. Time is short! Therefore it is extremely important that all political and religious differences be put aside and all groups opposed to REAL ID, and biometrics, pressure U.S. and state lawmakers with a common voice. Stopping REAL ID, biometrics and database linking benefits all U.S. citizens. A “fix” on this scale requires the greatest cooperation from the greatest amount of people. Although much has been said about religious freedom in this document, and especially Christian teachings, these issues touch every U.S. citizen. Republican, Democrat, Independent, liberal and conservative, all citizens love their freedom and do not want international organizations or tyrannical departments running the country and destroying constitutional liberties.

This is not just a, First Amendment, religious rights issue. The ACLU may be more concerned about privacy and preventing illegal searching of personal information. But, Fourth Amendment privacy rights are also essential to religious freedom. Stopping illegal searches, stops global database linking. Protecting religious freedom depends on states retaining control over DL/ID cards (Tenth Amendment)--- no national or international DL/ID. The Tenth Amendment limits federal powers and protects our access to the more “flexible” powers of state government, thus protecting our rights to representation on a local level. The right of representation is permanently damaged by this system since we have no representation with other nations or international organizations. Furthermore, once databases are linked, it is impossible to correct, making it impossible for a redress of grievances (First Amendment). So, our First Amendment religious rights are interconnected with other rights. All U.S. citizens share those rights. There is much room for common ground and agreement. However, we must be focused on the real solution that serves the common good.

We must stop biometrics, database linking-sharing and stop the influence of international organizations on U.S. law and government agencies.

Several things must happen to dismantle the biometric machine that has been growing since 1986. Below are some proposed solutions.

Nationally –

REPEAL REAL ID and other ID laws that depend on biometrics.

Wipe existing biometric information from passport, government employee ID records, military ID and related databases. Another possibility is to “permanently degrade” stored images so they are no longer usable with facial image recognition.

State level –

Wipe high-resolution facial images and any biometric fingerprints from existing DL/ID

databases.

Replace existing biometric equipment with non-biometric systems that is limited to low-resolution facial images (no more than 25 pixels between eye centers --- current biometric ICAO standard is 90 pixels between eye centers). The purpose of this change is to make images "human readable" not "machine-readable." This makes, existing and future facial images unusable for biometrics and pushes out the window for another "take-over" of state ID, at least 4-10 years, depending on the renewal cycle of each state. Using lower resolution images, even with sophisticated tamper resistant documents, will save this nation millions and millions of tax dollars that can be spent of REAL security. Based on vendor claims and actual results, states and federal agencies should consider financial recovery against biometric vendors that misrepresented their products to obtain contracts.

Permit residents to OPT-OUT of photo and/or Social Security Number retention by state DMV-DPS (NH Model). This makes the state database incomplete of photo images, making it far less valuable for biometric enrollment or federal take-over in the future. This also protects privacy. If state DL/ID cards are securely designed, states do not need to retain the information, once the card is issued.

Permit residents to use mailing addresses, instead of physical addresses (required by REAL ID).

States must decide what technologies are best for ID document security, but without biometrics or data storage technologies like RFID chips and 2-D barcodes.

ID "breeder" documents, such as birth certificates can be made more secure and verified directly with the issuing agency. We do not need a DHS or AAMVA database or information clearing-house.

Businesses and schools, using biometrics must notify workers, visitors, students, parents of students, etc. of its use of biometrics, and create non-biometric ID document alternatives for employees, students, etc.

Hospitals must notify, parents of newborn babies, of any biometric uses (no more ink) and provide a non-biometric alternative.

Nationally and on a state level –

U.S. citizens must reclaim their government from the influence of international organizations such as AAMVA and ICAO. Typically, lawmakers create legislation, and the appropriate department promulgates the regulations. However, the dangerous influence of AAMVA and ICAO, has infected state and federal agencies and must be stopped. We have no hope of correcting this threat unless the influence of such organizations is addressed and control over government agencies is restored.

DO IT –TIME IS RUNNING OUT

The mission of Christians and pastors should be to speak-up and oppose this threat. Many hesitate to do so because of the complexity of the subject. Don't speak of complexity. Speak your conscience. Does it threaten your beliefs to be enrolled in this system? If yes, then the law must be changed, not the belief. PERIOD.

Simply tell lawmakers (U.S. and state) that REAL ID, biometrics, database linking and the influence of international organizations over state and U.S. law, threaten your religious rights. You will be shocked. Many U.S. and state lawmakers do not know of these issues. It is up to you to tell them. Encourage them to contact lawmakers in other states that have successfully stopped REAL ID. Simple letters and emails to lawmakers send a huge message. Bring their attention to this overlooked issue and also confirm the threat to religious rights. These letters and emails DO NOT require technical knowledge, but the sincere voice of concern. Pastors are especially powerful. Their voice, in the mind of the lawmaker, represents dozens or thousands of voters. Aggressively, stand for your constitutional rights, or you will lose them

Pastors, tell your congregation. Protect them from this threat. People are available to educate. Short handouts and other materials can be distributed. Because many large Christian organizations have failed to address this issue, the international ID-biometrics-religious issues have largely been ignored in the mainstream. Individuals and pastors must petition these large organizations and their own denominational headquarters to immediately oppose this issue. Today, several groups, Senators, Congressman, state lawmakers, etc. have the information now and are investigating it with great concern. God is on our side.

REFERENCE PAGE

- ⁱ Source AAMVA – “Current and Ongoing Efforts – <http://www.aamva.org/KnowledgeCenter/Standards/currentandongoingefforts-biometrics.htm>
- ⁱⁱ Source ICAO – Tag/Mrtd17_WP016.pdf (Jan. 2007) “Background 2.1”
- ⁱⁱⁱ Source DHS – “Notice of Proposed Rulemaking” (Mar. 2007) – section 3 “Digital Photograph” (March 2007) footnote (17) states “*The relevant ICAO standard is ICAO 9303 Part 1 Vol 2, specifically ISO/IEC 19794-5 - Information technology - Biometric data interchange formats - Part 5: Face image data, which is incorporated into ICAO 9303*” nprm_readid.pdf
- ^{iv} Source AAMVA web site – www.aamva.org and listed on other source documents (see note i – Current and Ongoing Efforts – <http://www.aamva.org/KnowledgeCenter/Standards/currentandongoingefforts-biometrics.htm>)
- ^v Source AAMVA - <http://www.aamva.org/KnowledgeCenter/Driver/Compacts/History+of+the+DLA.htm>
- ^{vi} Source AAMVA – std2005DL-IDCardSpecV2FINAL.pdf
- ^{vii} Source H.R.418 REAL ID ACT of 2005 – Sec. 203 “Linking of Databases” – re: “Driver License Agreement” //NOTE: HR418 from House was included in HR1268 in Senate, passed and signed into law
- ^{viii} Source DHS – “Notice of Proposed Rulemaking” (Mar. 1st 2007), “H. Minimum Driver’s license or identification card Data Element Requirements - Sec. 5 Signature, Sec. 8. Machine Readable Technology (MRT) barcode standard, data elements, Sec. 9 Encryption (barcode) J. Source Document Retention (and related sections detailing these requirements) - nprm_readid.pdf
- ^{ix} ICAO announces (July 11th 2005) the Machine Readable Passport (MRP) standard specified by ICAO is the international standard -- pio200507_e.pdf
- ^x “Enhanced Border Security and Visa Entry Reform Act of 2002” “Sec. 303 Machine Readable Tamper Resistant Entry and Exit” requires biometric Machine Readable Passports, complying to ICAO standards, for “visa waiver nations.”
- ^{xi} Source ICAO – Tag/Mrtd17_WP016.pdf (Jan. 2007) 3.1 Creation of ICAO
- ^{xii} Source ICAO – Tag/Mrtd17_WP20.pdf (March 12th, 2007) “2. ONGOING WORK OF THE NTWG SINCE TAG/16” sec. 2.2

- ^{xiii} Source DHS – (See ref. iii) - The ISO/IEC 19794-5 standard defines how photos, compatible with facial recognition biometrics, are to be collected when used in ICAO’s 9303 Machine Readable Travel Documents (MRTD).
- ^{xiv} ICAO 9303 - ISO/IEC 19794-5 is available from ISO (see 040607 April_6_FP_Published_ISO_Standards.pdf), however, “Annex D-Face Image Data Interchange.pdf” addresses similar content and can be downloaded.
- ^{xv} Source DHS – “Notice of Proposed Rulemaking” (Mar. 1st 2007), “Sec. 6. a, ii. Federated Querying Service - nprm_readid.pdf
- ^{xvi} Source DHS - Privacy Impact Assessment for the REAL ID ACT of 2005- Sec. 3 “The State to State Data Exchange” (footnote 24) refers to AAMVAnet as one part of a current data exchange program that could be used to implement the requirements of REAL ID’s database linking requirements – privacy_pia_realid.pdf
- ^{xvii} Source DHS – http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm
- ^{xviii} Source Wall Street Journal Article July 8th, 2005 “Surveillance Cameras Monitor Much of Daily Life in London May Help to Identify Bombers” - http://online.wsj.com/public/article/SB112077340#647880052-cKyZgAb0T3asU4UDFVNPWrOAqCY_20060708.html
- ^{xix} Source ICAO – TagMrtid17_WP016.pdf – 5.3 SELECTION OF BIOMETRICS MODALITIES FOR E-PASSPORTS
- ^{xx} Source Washington Technology – Great Expectations – Biometrics – http://www.washingtontechnology.com/print/18_13/21791-2.html
- ^{xxi} Source AAMVA IBG Report - UID9BiometricReport_Phase1_1to300m.pdf
- ^{xxii} Source FRVT2006andICE2006LargeScaleReport (4).pdf <http://frvt.org/FRVT2006/default.aspx>
- ^{xxiii} Source Washington Post (Sept. 18th 2007) “DHS ‘Dry Run’ Support Cited” <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/17/AR2007091701718.html?hpid=moreheadlines>
- ^{xxiv} Source AP “Glitch Renders ‘Virtual Fence’ Unusable (Sept. 20th 2007) – <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/19/AR2007091902664.html>
- ^{xxv} Source USA Today - Phoenix test site for TSA X-ray - http://www.usatoday.com/printedition/news/20061201/1a_lede01.art.htm
- ^{xxvi} Source DHS- Deception Detection: Identifying hostile intent – <http://www.homelandsecurity.org/snapshots/newsletter/2007-05.htm#deception>
- ^{xxvii} Source GCN –DHS pushes global data sharing – http://www.gcn.com/print/26_03/43061-1.html

A brief list of laws, initiatives and treaties being used to impose a global biometric ID system

The “**Commercial Motor Vehicle Safety Act of 1986**” attempted to impose biometrics on state ID for identifying commercial driver’s license holders

1995 ICAO began work on biometric Machine Readable Travel Documents (MRTD’s) resulting in ICAO 9303 TAG-MRTD/17-WP/16.pdf (1-6-07)

The “**Illegal Immigration Reform and Immigrant Responsibility Act of 1996**” set federal standards for all driver’s license/ID cards (DL/ID cards) and placed state DL/ID card design under the influence of AAMVA

“**Enhanced Security and Visa Reform Act of 2002**” – biometrics collected on visa holders - Visa Waiver nations issue biometric passports designed by ICAO

REAL ID ACT of 2005 and **NPRM** require states to:

1. Collect, store and share highly personal information verified through online systems (ex. DHS “federated querying” system or AAMVAnet)
2. Adopt global biometric DL/ID card standards set by AAMVA and ICAO “9303” photo standards complying with “**biometric data interchange formats**” making all photos compatible with facial recognition software
3. Link state DL/ID databases, creating common database systems (DLA model) – Once databases link, the photos can be accessed by government agencies outside the state. The images can then be used with common facial recognition systems. State database linking and information sharing permanently enrolls U.S. citizens in a global biometric system. Data cannot be retrieved once distributed. The shared data can then be shared globally as part of an international database linking system.

Initiatives – WHTI (Western Hemisphere Travel Initiative) requires a passport for travel between Canada, United States and Mexico as of 2007– WHTI meant new applicants issued new biometric e-passports (ICAO design). DHS began pilot program with Washington, Arizona and New York to issue biometric DL/ID card/passport hybrid acceptable as passport. **TWIC** (Transportation Worker Identification Credential) - Requires biometric ID cards for thousands of government employees

July 2007, the EU and US begin sharing new database information on travelers, including “*racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership*” and “*data about an individual's health, traveling partners and sexual orientation*” according to a July 27th, 2007 Washington Post article. Such data collection and sharing depends on other federal laws, like the recently revised FISA, to permit surveillance and data mining of information on U.S. citizens. Robert Moczyn (DHS-US Visit) stated that global data sharing would begin with Europe, Asia (GCN February 5th, 2007).

Bodily Integrity Act

An act prohibiting forced implantation of identification and tracking devices in individuals

DEFINITIONS

"Entity" means an individual, corporation, business trust, estate, trust, partnership, limited liability corporation, association, foundation, joint venture, government, government subdivision, agency or instrumentality, public corporation or any other legal or commercial entity.

"Individual" means a unique, separate human being.

"Identification/Tracking Device or Mark" means any item, application, device, marking, or other technology capable of storing or passively or actively transmitting an individual's identity, characteristics, status, group membership, travel history, or location, or capable of storing or transmitting a number, symbol, signal, pattern, or other identifier that could be linked with any such information.

"Track" means to locate, follow, monitor.

"Discriminate" means to make distinctions, have bias, prejudice, or partiality.

PROHIBITIONS

Requiring Human Identification/Tracking Device or Mark Prohibited

No entity shall require, coerce, or cause an individual to have an identification/tracking device or mark implanted or permanently or semi-permanently incorporated into or on the body, skin, teeth, hair, or nails of that individual.

Consent

In no instance shall an identification/tracking device or mark be implanted or incorporated into or on the person of an individual without that individual's informed written consent, with full disclosure of any health or other risks associated with the device or mark.

Consent of a guardian, guardian ad litem, attorney-in-fact, parent or other agent shall not be considered adequate consent.

The individual undergoing implantation or incorporation of an identification/tracking device or mark must be at least eighteen years of age and of sound mind to grant consent.

Implanting Identification/Tracking Device or Mark in the Deceased Prohibited

In no instance shall an identification/tracking device or mark be implanted or incorporated into or on a human corpse.

Identification and Tracking Prohibited:

No entity may use an identification/tracking device or mark in or on the person of an individual to identify that individual or as a means of, or aid to, tracking that individual, without the consent of the individual being identified and/or tracked.

Discrimination Prohibited:

No entity shall use the absence of an identification/tracking device or mark as a basis for discriminating against an individual for any purpose whatsoever, including, but not limited to, employment, housing, insurance, medical care, voting, education, travel, banking, finance, and commerce.

Penalties

[To be determined by the legislature]

To request expert testimony related to this bill or other issues related to RFID and human implantation, please contact Dr. Katherine Albrecht, Director of CASPIAN Consumer Privacy www.AntiChips.com

Pennsylvania Model Legislation

The following is the "model" provided by Rep. Sam Rohrer of Pennsylvania, who has introduced HB 1351 in response to the need to address Real ID for the Commonwealth. As printed below, it represents the changes agreed to by Rep. Rohrer in consultation with Larry Frankle (ACLU Lobbyist), James Compton (AFTF State Coordinator) and Aaron Bolinger (NVCCA Legislative Director/Theologian) in meetings designed to strengthen the bill in committee and as a model for other states.

AN ACT

Relating to compliance with the Federal REAL ID Act of 2005 & other laws impacting biometric and economic privacy.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Short title.

This act shall be known and may be cited as the Pennsylvania REAL ID Act.

Section 2. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Biometric data." Information relating to a biological characteristic of an individual that makes that individual unique from any other individual, including, but not limited to, the following:

- (1) Fingerprints, palm prints and other means for measuring or recording ridge pattern or fingertip characteristics.
- (2) Facial feature pattern characteristics.
- (3) Behavior characteristics of a handwritten signature, such as shape, speed, pressure, pen angle or sequence.
- (4) Voice data used for comparing live speech with a previously created speech model of an individual's voice.
- (5) Iris recognition data containing color or texture patterns or codes.
- (6) Keystroke dynamics, measuring pressure applied to key pads.
- (7) Hand geometry, measuring hand characteristics, including the shape and length of fingers, in three dimensions.
- (8) Retinal scans, reading through the pupil to measure

blood vessels lining the retina.

- (9) Deoxyribonucleic acid or ribonucleic acid.

"Economic privacy." The privacy of an individual that relates to a right, privilege or reasonable expectation that certain information is required by law to be held confidential or is otherwise considered to be confidential to that individual, including, but not limited to:

- (1) Information included in a tax return required by law to be filed with the Federal, State or a local government.
- (2) Information on financial transactions conducted by or on behalf of the individual.
- (3) Information of investment transactions conducted by or on behalf of the individual.

"REAL ID Act of 2005." Division B of the Emergency

Supplemental Appropriations Act for Defense, the Global War on Terror and Tsunami Relief, 2005 (Public Law 109-13, 119 Stat. 302).

Section 3. Participation in the REAL ID Act of 2005.

Neither the Governor nor the Department of Transportation or any other Commonwealth agency shall participate in the compliance of any provision of the REAL ID Act of 2005.

Section 4. Participation in other related laws.

Neither the Governor nor the Department of Transportation or any other Commonwealth agency shall participate in the compliance with any federal law, regulation or policy that

would compromise the economic privacy or biometric data of any resident of this Commonwealth.

Section 5. Legal challenge.

Either the Governor or the Attorney General may file an action in a court of competent jurisdiction to challenge the constitutionality or legality of the REAL ID Act of 2005.

Section 6. Effective date.

This act shall take effect in 60 days.