

Position Paper

Airline Passenger Management System (APMS)

Prepared by: Rodrigo A. Guajardo
InfoTrek Creative Project Solutions

January 2003

Recipient: Nicholas J. Naclerio

Confidentiality Notice

This full document is privileged and confidential and is intended only for the use of the person named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.

Topic Background: Enhanced Airline Security.

Independent experts and key members of Congress recognize publicly that America's airline security system is in disarray, and the Transportation Security Administration, created in the aftermath of Sept. 11, faced two deadlines to install key air-security measures by the end of 2002 that could not meet as every outside expert prognosticated, as the Salt Lake Tribune Reported on Saturday July 20, 2002.

The agency performed so poorly that its boss was fired on July 18, 2002. The agency now is out of money and it had been borrowing funds from another federal agency that no longer shells out the stopgap loans. "TSA has become a monster," said Rep. John Mica, R-Fla., chairman of the House of Representatives Aviation Subcommittee.

Problems facing the TSA, include:

- Within four months of the agency's foundation, under a deadline set by law, the government should have taken over all airport passenger-screening sites, hiring federal workers to check for weapons. So far the TSA did this in only three out of 425 airports by the end of 2002.
- All checked bags should have been able to be screened for explosives by Dec. 31, 2002, but the TSA had deployed only 226 of the 5,900 screening systems needed to accomplish this monumental task. Previously to this, and recognizing that the deadline was unlikely to be met, the House Select Committee on Homeland Security voted on Friday July 19, 2002 to extend it by one year, and the delay was attached to the legislation to create the new Department of Homeland Security.***
- Commercial cargo in passenger jets is not being checked adequately and satisfactorily for bombs, explosives, or other analogous threats.
- Screeners failed to detect 1 in 4 mock weapons, on average, in 387 tests performed at 32 airports before July 2002. "This is particularly troubling, because undercover officers probing the system were instructed not to make dummy weapons difficult for screeners to find," the same House memo said.
- Lawmakers aren't the only ones who see problems with airline security. "Billie Vincent, a former Federal Aviation Administration security chief, said the current TSA-run system was "an undisciplined mess." *** "They were overwhelmed, understaffed and wrongly positioned to accomplish everything that was thrown at them," said Lou Tyska, chairman of the transportation security committee for the American Society for Industrial Security, a trade group of corporate security chiefs. "They were doomed to failure."

We hear so much about new devices to better screen passenger luggage for bombs and other threats. What we don't hear however, is how better to secure our airlines from potential internal sabotage or to ***extend proper and effective protection to passengers in flight.*** What is being done to screen those who have easy access to the planes - the ground crew and support personnel? Undercover investigations have shown newly hired ground crew (hired by the way - without any background check) has free access to roam empty planes sitting on the tarmac. Until safeguards are put into place whereby the ground crew and ALL support personnel (i.e. food handlers, cleaning crew, mechanics, etc.) are carefully screened

Confidentiality Notice

This full document is privileged and confidential and is intended only for the named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.

before they have access to any plane - we are only taking care of 1/2 of the problem. **This leaves an open door to transfer the risk to the plane in flight.**

After Pan Am Flight 103 exploded over Lockerbie, Scotland on December 21st, 1988, you would have thought that any nation that could afford it would spare no expense in ensuring that such an event could never occur again. If any nation could afford anything, it's the United States.

Yet as has come to light in the aftermath of September 11, thirteen years after Lockerbie, checked baggage was still not being adequately screened for explosives in the United States, and passenger screening is still a mayor problem..

In KOCHI, India, the Bureau of Civil Aviation Security (BCAS) Commissioner, Veeranna Aivalli, has said that the process of security in the aviation sector can be smoothened and eased only by proper segregation of passengers. A **scientific segregation** of passengers **within the plane** based on their personal history and using **Biometrics identifiers** will certainly help the security personnel concentrate on a few who can be included in the 'suspect list', he said.

India was the worst affected country in the world with regard to airline hijacks. Between the first hijack that took place in January 1971 and the last hijack of an Indian Airlines flight to Kandahar a couple of years ago, the country had suffered 25 times. Among the 27 hijacks in the country so far, 17 flights were of Indian Airlines.

Who knows who s on the plane?

In its efforts to anticipate or prevent crimes, the FBI must at times initiate investigations in advance of criminal conduct. Currently, the FBI has a state of the art, on-line computer database known as the Terrorist Information System (TIS) containing information, **ranging from text to Biometrics**, on suspected terrorist groups and individuals. The system has over 200,000 individuals and over 3000 organizations or enterprises. The individuals indexed include subjects of investigations and known or suspected members of terrorist groups, associates, contacts, victims and witnesses. The organizations or enterprises include not only terrorist groups but also affiliated organizations or enterprises. However, currently TIS does not allow the FBI to rapidly cross-reference, build a suspect profile and retrieve its information, and to make links between persons, groups or events with the field (i.e.: airports, planes, hospitals, museums, federal agencies, public places, etc.). These systems are not in place, thus making the FBI and law enforcement work ever more difficult.

Also, there appears to be a growing problem of disaffected loners who cut themselves off from all groups. An increased effort to monitor anti-government groups is unlikely to identify these loners, mainly because of lack of biometrical and historical information, who may pose the greatest threat, specially if they are on board of an airplane, and moving at glance.

Using Biometrics raises some complicated legal, ethical, and sociological issues, specifically on how to safeguard biometric information so it cannot be used for other, possibly nefarious, or illegal purposes. Although no significant legal obstacles bar anyone from establishing a biometrics program in the United States, valid sociological concerns exist, for the most part in the area of privacy, but these concerns can be easily addressed by existing local and State regulations (minimally) and by installing additional and specific safeguards.

Confidentiality Notice

This full document is privileged and confidential and is intended only for the named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.



On Wednesday, January 29, Australia launched the world's first automated passport checks using facial-recognition technology on as it continued to tighten security at its borders in the aftermath of the September 11, 2001, attacks. The new SmartGate kiosk scans passport photos and compares them with the faces of travelers -- replacing manual checks by customs officers at Sydney airport. The first phase of the project will apply only to crewmembers of national flag carrier Qantas Airways Ltd. Later, It will be expanded to passengers, and staff of other international airlines, and other Australian airports, by 2004.

Until Mohammed Atta stood up on American Airlines flight 11 and shouted, "This is a hijacking, he wasn't a criminal, nor did he have any criminal records on file." Currently, the entire airline passenger clustered, non-linked ID profiling systems are unable to stop hijackers. Once the hijacker or terrorist is on board, it is very little or nothing that can be done to stop another massacre.

⊗⊗⊗

Privacy Issues

Although the word privacy does not appear in the U.S. Constitution at all, concerns on the subject of protecting citizens in opposition to government infringement into their private territory is echoed in several of its provisions. Three principal sources deal with legal rights to privacy: federal and state institutions, the common law of torts, and statutory law.

The Privacy Act of 1974 is a well-known sample of legislation controlling the use of personal information by the federal government. By and large, the Act prohibits the federal government from disclosing personal information without the express consent of the person who provided it.

The Fourth Amendment protects against unreasonable searches and seizures, and the Supreme Court has explained that government action constitutes a search when it invades a person's reasonable expectation of privacy. However, the Supreme Court has also determined that a citizen does not have a reasonable expectation of privacy with regard of physical characteristics that are constantly exposed to the public, such as one's facial features

The APMS works well within the frame of law.

⊗⊗⊗

Confidentiality Notice

This full document is privileged and confidential and is intended only for the person named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.

Position.

I strongly recommend the use of the **Airline Passenger Management System (APMS)**, a smart belt capable of scheming in-flight fare flow dynamics by assessing, managing, and controlling the traffic of passengers that can pose a potential risk, by means of restrain. The need for the APMS, assisted by intelligent historical and biometrical data on board airplanes is imperative, and the need for this system is long overdue. The APMS system will efficiently deter and prevent criminal acts against airplanes; will effectively help in protecting the life of passengers, aircrew and pilots, and will certainly help to safeguard the planes themselves.

The use of the APMS can also set the basis to conduct to a needed development of standardized methodologies and decision aid tools for vulnerability analysis and enhanced passenger protection for this critical element of our nation's security infrastructure: our airlines. The nationwide implementation of APMS will provide a dependable and reliable security system to effectively prevent the risk of hijacking while in flight.

⊗⊗⊗

Confidentiality Notice

This full document is privileged and confidential and is intended only for the use of the person named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.

Strategy.

The implementation strategy for APMS will vary from case to case depending on several factors such as airport traffic, local and State regulations, technology availability, cross reference points, and level of security required. However the APMS implementation will serve any airport, and will provide an interoperable base for security.

The APMS consists of an internal computer network in the airplane with a hard-wired connection to every passenger seat. A display panel in the cockpit and the passenger compartment indicates and keeps track of the status of each passenger seat as to occupancy, and the status of each smart seatbelt. The panels indicate one of the following statuses: unfastened, fastened, loosely fastened, locked, and unlocked. Only the APMS can lock and unlock the seat belt.

The system is programmed so that no passengers are authorized to leave their seat during certain stages of the flight. To ensure compliance all seat belts are locked. When passengers are authorized to leave their seat their numbers is limited to a predetermined percentage of the total passenger load, based on the intelligence gathered by the system through Biometrics. Passengers are classified according to the risk they present and the computer program ensures that only one high-risk passenger is allowed to move around the cabin at any particular time. The system is also capable to alert Air Marshals when a red flag is activated by APMS, so passengers are granted permission to walk around the cabin in accordance with their place in the computer managed queuing system, which considers the order along with the risk level of the passenger. All other passengers remain locked in their seats with their seat belts fastened.

Collecting Biometrics.

The passengers Biometrics data collection will occur at the check-in stage (in a more advanced settings, this data gathering can occur at the time the airplane tickets are bought). To ensure positive identification, three levels of aggregation can be used: i.e.: iris scanning, digital mug shot, and voice pattern. These Biometrics than can be cross-referenced with current local data banks for validity, and integrated into a bar-code system to provide a combined three-points reference data. The data now is encoded or encrypted, and free of contamination. This data can be used now to authenticate who s boarding the plane, provide needed intelligence for passenger traffic, provide a cross-reference point at both, the arrival airport, and the custom points. In other words, APMS can authenticate that the same passenger that boarded the plane, is the same that is unloading. There are cases where a male passenger leaving an airport, arrives as a female at the end destination.

The APMS can also download the passenger s data at the arrival airport s system. This will increase the security at checkpoints, and provide data to local authorities, which in turn, can scan for sought criminals or terrorists.

Using Biometrics

The proper use of Biometrics will quickly resolve a situation such this one:

Confidentiality Notice

This full document is privileged and confidential and is intended only for the person named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.

Two people arrive to an airport. Although both are terrorists, one has no criminal records; the other does. The person without criminal records buys a ticket and obtains a boarding pass. Then, the known terrorist uses the ticket, the boarding pass, and an easily obtainable set of false identifiers emulating the data captured on the plane ticket and boarding pass. When he goes through the checkpoint, the security personnel have no way to positively authenticate or validate the identifying documents the passenger carries. Security personnel do not have ready access as well to data matching this known terrorist (we learned this on 9-11). He carries no visible or identifiable weapons on him or on his luggage, so he passes the security checkpoint undetected. We all know that it is not necessary to have weapons to bring a plane down. Now we have a terrorist on board and a tragedy waiting to happen.

The APMS equipped with biometrics can perform a real-time, or a close to real-time cross-reference check of the identifiers. The system can use a secured and updated mirror site from the Division of Motor Vehicles (DMV) to check the driver's license; the same infrastructure can be used with the Passport Office, the FBI's TIS or NCIC, thus providing a secure, updated, and independent source of authentication. The voice patterns can also be stored and ready available as a third source of authentication. The degree of aggregation will directly and dramatically impact on one's ability to use false documentation, or gain advantage from identity theft.

Once this is done, the data on the flight manifest as well as the Biometrics data of the passengers is uploaded into the computer by Ground Operations just before take off. This will allow passengers with special needs, or medical conditions to be easily identified and cleared in advance and then be given preferential treatment by the system. The Flight Attendants or an Air Marshal can access this information using hand held (wireless) devices by simply entering the passenger's seat number. In addition, the Flight Attendant can communicate with the Pilots and Ground Operations using the hand held device. The Flight Attendants are not able to unlock seat belts using these devices.

Immediate Collateral Benefits

APMS not only provides a safe and reliable security and deterrent system in the airplane, but also sets the basis for a preventive anti-terrorist, anti-criminal system for the entire flying industry. Criminals will know that as soon as they get involved in the airport system (or any airport equipped with the system), they will be detected, and consequently arrested and prosecuted. APMS will make virtually impossible for criminal perpetrators to deliver terrorist acts, and will inflict a tremendous blow to their capacity to mobilize. The APMS is an open-end system that can be adapted to support and assist other countermeasures already in use.

⊗⊗⊗

Confidentiality Notice

This full document is privileged and confidential and is intended only for the use of the person named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.

Corporate Background

For the past 10 years, InfoTrek Creative Project Solutions has actively explored the fields of Biometrics. By doing this, we have accumulated a tremendous expertise in the application, implementation, management, and statistical deviation of its results. Previous to that, our expertise goes back to early 1974 when we directly assisted the Chilean government with fundamental Biometrics recognition processes to identify, track and observe traffic control for military personnel and civilians after the military coup of September 11, 1993, to prevent and counter terrorism infiltration.

In spite of InfoTrek's active long time efforts to make the government and the Law Enforcement community aware of the valuable benefits of and identification systems based on Biometrics to combat crime and terrorism previous to the 9-11-2001 incidents, our preaches have not been heard. This is another case (APMS) where perhaps more close attention shall be put to counter terrorism and crime, and save U.S. citizen's lives.

InfoTrek has been involved in very high consequence systems most notably such as a Biometrics-based forensic software developed for the FBI and local and State Law Enforcement use to track stolen property and hunt down and capture criminal perpetrators. Over the years, the resulting best practices have been examined to construct a strategy for commercial applications and government agencies to address complex security challenges of the 21st century, including the following:

- Manage integration and increasing complexity of interdependent systems
- Counter physical terrorism traffic
- Assure no terrorism yield by accident or hostile intent
- Counter the potential for terrorism infiltration
- Assure a dependable infrastructure "where things work."
- Provide solutions for aging scattered, non-linked Biometrics systems
- Assure a safe, secure, and reliable Biometrics cross reference system
- Provide for a multi-access, multi-platform able system
- Counter crime
- Counter terrorism
- Provide safer and secure schools
- Advance solutions for Biometrics reliability, safety and security
- Provide solutions for aging infrastructure

The increasing complexity and interdependence of these emerging challenges, and the immediate urgency they pose stimulated the development of a new Biometrics strategy for the nation. InfoTrek can examine and expand the conceptual methodology to test its potential application to broader national challenges and needs. The results will assist the agencies responsible for those issues in communicating, if they desire to do so, and in providing clear issues and potential Biometrics solution applications.

⊗⊗⊗

Confidentiality Notice

This full document is privileged and confidential and is intended only for the named above. Any unauthorized copying, distribution, disclosure, or other use of the contents of this document is strictly prohibited. The privileged nature of this document shall not be waived by the review of this document by anyone other than the intended recipient.