Steering Committee Analysis

November 16, 2001

DoD Counterdrug Technology Development & NIJ (Co-chair)
Federal Aviation Administration (Co-chair)
Technical Support Working Group
National Institute of Justice
White House Office of National Drug Control Policy
U.S. Customs Service
Defense Advanced Research Projects Agency
Federal Bureau of Investigation

Executive Summary

One of the most commonly recommended technology areas for improving aviation security is biometrics. The FAA and many other Federal agencies have been performing research, development and evaluation of these technologies. The purpose of the Aviation Security Biometrics Working Group was to bring together representatives of these Federal Agencies, combined with information gathered from government, industry, and academia, to develop a systematic, comprehensive concept of operations for the application of biometrics in aviation security.

The biometrics industry is on the threshold of providing a major infusion of new technology into the American way of life. The Working Group studied the efficacy of incorporating biometric technology into aviation security. Within the aviation security realm, there are four distinct application opportunities:

1. Employee identity verification and access authorization.
2. Protection of public areas in and around airports using surveillance.
3. Passenger protection and identity verification.
4. Aircrew identity verification (ground and in-route).

Each of these applications has different considerations regarding the selection and use of biometrics. Discussion of this topic often gets confused if this distinction is not clear. They each also will have commonality and interactions with other security applications that could provide mutual benefits.

1. Introduction

1.1 Working Group Structure

As part of its continuing efforts to increase the security of airports within the United States, the FAA established a multi-agency working group to accelerate its study of the integration of biometrics into airport security systems. The Aviation Security Biometrics Working Group (ASBWG) is co-chaired by the DoD Counterdrug Technology Development Program Office and the Federal Aviation Administration and is being organized by a Steering Committee made of Program Managers from eight different federal agencies. Four Focus Groups were established, consisting of representatives of government, industry, and academia, to gather information for submittal to the Steering Committee. The Steering Committee analyzed the data provided from the four Focus Groups and developed the recommendations given in this document. A description of the four Focus Groups, their threats to be addressed, and their goals as first defined are described in the following subsections. Some Focus Groups modified their threats and goals after discussion (see Chapter 2).

1.1.1 Employee Identity Verification and Access Authorization[1].

Using biometrics devices to recognize employees provides a means to ensure access to secured areas within an airport is restricted to authorized personnel. Biometric devices are considered as only one essential component of a more effective access control system, with other integrated system components needed to detect and prevent unauthorized access.

Threats to be addressed

- Unauthorized access utilizing:
    - Lost or stolen ID cards (or keys, pin codes, cipher codes)
    - Covert tailgating (employee unaware)
    - Collusion piggybacking (employee aware)
- Authorized access by insider turned terrorist (on watchlist)

Security System Goals and Objectives

- Restrict access to secured areas to positively identified, authorized individuals

1 The Biometrics for Positive Recognition of Employees Focus Group consisted of:
ONDCP, Facilitator
Alaska Air
Avanti
Department of Transportation/Volpe Center
NAVSEA Crane
GSA Smartcard
UK Biometrics Working Group
San Jose State University

- Handle the movement of large objects (oversize bags, carts) that must pass through
- Consider provisions for "escorting" of un-enrolled individuals or groups
- Provide "universal access" for flight crews using one ID for authorized entry at multiple sites
- Promote integration with control devices to detect and control (or respond to) piggybacking or tailgating

1.1.2 Protection of Public Areas In and Around Airports Using Surveillance[2].

Facial recognition, as well as other biometric technologies currently under development, shows significant potential for combating terrorism via controlled and general surveillance. Controlled surveillance occurs at locations were the movement of people, lighting, and pose of a can be controlled. General surveillance could occur at locations where these factors cannot be controlled.

Threats to be addressed

- Terrorists on watch lists (TOWL) entering the country by air travel
- Presence of TOWL in or near airport (public areas)
- TOWL attempting to pass through as a passenger
- TOWL in vehicle approaching airport (potential attack, suicide bomber, etc.)

Security System Goals and Objective

- Detect TOWL upon arrival, attempting departure, or in/around/approaching airport
- Automate recognition decision making to the maximum extent possible
- If TOWL is detected (or possible hit), heighten surveillance for known accomplices

2 The Protection of Public Areas In and Around Airports Focus Group consisted of:
DARPA (Facilitator)
Shafer Corporation (Co-Facilitator)
Stanford University
Lau Technologies
Visionics Corporation
UK Home Office
Federal Bureau of Investigation

1.1.3 Passenger Protection and Identity Verification[3]

Biometrics could be used to positively verify the identification of all passengers who board an aircraft. This application is complex and controversial because of high volume and privacy concerns. The concept calls for enrolling passengers in a national travel identification system. Identity verification could take place at check-in, security checkpoint, boarding, baggage claim, customs, and immigration. Either a centralized database or biometric templates stored on smart cards will be necessary to enable distributed identity verification.

Threats to be addressed

- Terrorist on watch list attempting to register for Aviation Security Identity Recognition (ASIR) program (identity deception)
- Someone trying to use another's identity to board a plane (identity theft)
- Air carrier identified undesirable/prohibited individuals (air rage offenders)

Security System Goals and Objective

- Prohibit air travel by undesirables and Terrorists on Watch Lists (TOWL)
- Minimize impact of security on normal passenger's travel experience
- In the future, analyze travel histories to detect suspicious deviations or patterns

3 The Passenger Protection and Identity Verification Focus Group consisted of:
DoD CDTDPO, Facilitator
Alaska Airlines
Avanti
NAVSEA Crane
International Air Transport Association
GSA Smartcard
Federal Aviation Administration
Walt Disney World
International Biometrics Industry Association
BioAPI
San Jose State University
RAND
Federal Bureau of Investigation

1.1.4 Aircrew Identity Verification (Ground and In-Route)[4].

Biometrics might be used to positively verify flight crews prior to boarding the aircraft, as well as continuous verification throughout the flight. This concept could also be extended to FAA air traffic controllers and others in key positions in the airspace information infrastructure.

Threats to be addressed

- Hostile take-over of control of an aircraft
- Impersonation of a pilot by a terrorist
- Unauthorized air traffic controller in control

Security System Goals and Objective

- Positive identity verification of pilot, co-pilot and crew prior to taking control of the aircraft
- Periodic verification of the identity of the pilot in control, in the seats
- Possibly extend into detection of duress or stress in the pilot
- Need system to verify aircraft "health" in addition to aircrew identities. Change in aircraft health should trigger aircrew identity re-verification

1.2 Aviation Structure Overview

Within the United States, there are over 400 airports in six categories covered by the FAR 107, airport security. Categories are determined mostly by traffic volume, nature of traffic, threat assessment, and law enforcement response time required.

Category Type	Makeup
Cat X	21 of the highest threat/risk
Cat I	60
Cat II	51
Cat III	135
Cat IV	169
Cat V	11

4 The Aircrew Identity Verification Focus Group consisted of:
National Institute of Justice, Facilitator
Avanti
SPAWAR Systems Center Charleston
NASA
Federal Aviation Administration
Air Lines Pilots Association
International Biometric Industry Association
U.S. Air Force Rome Laboratory
Sandia National Lab

All US Airports are owned and operated by a local governmental entity and not the federal government. Legislation currently being debated in Congress could turn the oversight or operation of the security to the federal workforce. The Federal Aviation Administration has established nine regions throughout the United States to provide a field, corporate perspective to policy formulation, operations and delivery of FAA services to the customer. The regions play an important role in outreach with the community, Congress and the media, and are a strong promoter of aviation education.

Each airline has its own reservations system for booking passengers onto flights. Some airlines have integrated their systems with a network booking system (e.g. SABRE), but many smaller/regional carriers operate totally independently.

The FAA, its regions, airlines, individual airports and law enforcement agencies are not connected via dedicated network.

1.3 Biometrics Industry Overview

Biometrics are automated methods of recognizing a person based on physiological or behavioral characteristics. Examples include:

- Fingerprint
- Hand Geometry
- Iris Recognition
- Face Recognition
- Speaker Recognition
- Dynamic Signature

In general, biometric devices can be explained with a three-step procedure.

1. A sensor takes an observation. The type of sensor and its observation depend on the type of biometrics device used. This observation gives us a "Biometric Signature" of the individual.

2. A computer algorithm "normalizes" the biometric signature so that it is in the same format (size, resolution, view, etc.) as the signatures on the system's database. The normalization of the biometric signature gives us a "Normalized Signature" of the individual.

3. A matcher compares the normalized signature with the set (or sub-set) of normalized signatures on the system's database and provides a "similarity score" that compares the individual's normalized signature with each signature in the database set (or sub-set).

What is then done with the similarity scores depends on the biometric system's application.

This Biometric Methodology establishes the analysis framework with tailored algorithms for each type of biometric device. Face recognition, for example, starts with a picture, attempting to find a person in the image. This can be accomplished using several methods including movement, skin tones, or blurred human shapes. The face recognition system locates the head and finally the eyes of the individual. A matrix[5] is then developed based on the characteristics of the individual's face. The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison). This matrix is then

compared to matrices that are in a database and a similarity score is generated for each comparison.

Different biometric technologies are at differing stages in the life cycle. Fingerprint recognition, for example, is fairly mature for the law enforcement identification application due in large part to the FBI's IAFIS program. Fingerprints, along with other biometrics types, are not seen as mature for other applications. Within the next five to ten years, industry watchers anticipate biometric technologies will move into its maturity stage where revenues are stable and industry practices are set.

The market for biometrics, although increasing, was small compared to current sales anticipation to the aviation industry. Biometrics vendors are intensely competitive and are expected to continue this tradition. Likewise, only recently have government organizations taken a close look at the efficacy of these technologies to address legitimate security concerns. Consequently, there

5 A "matrix" is a rectangular array of numbers, similar to a numerical version of word search puzzles.

have been very few attempts at accurately gauging the overall state of the art for the technology, and very few aviation-specific evaluations performed by non-vendors.

An introduction to the different types of biometric technologies and performance measures is presented in Appendix A.

2. Steering Committee Analysis

The Steering Committee is pleased with the work the four Focus Groups have performed. Furthermore, the Steering Committee believes that biometrics are applicable in each of these four areas of study to ensure the greatest level of security possible. The Steering Committee also understands that implementation of some of the applications described in this documents would cause some privacy concerns by the public as well as fiscal concerns by Congress or the local implementing authority. Weighing the potential benefits of these applications against these concerns is beyond the range of expertise of the collective organizations involved in this Working Group. The debate caused by these issues will have to be discussed in open public forums, and solved at the Administration and Congressional levels.

This chapter provides a brief overview of the Steering Committee's technical and operational assessment of incorporating biometric technology into aviation security and is divided into sections for each of the four Focus Groups.

2.1 Employee Protection - Identity Verification and Access Authorization.

Airport and air carrier employees must have access to certain otherwise restricted areas in order to perform their jobs. Biometrics could be installed into access control systems to verify that any individual attempting to enter a secure area is the authorized individual.

2.1.1 Concept of Operations

The general concept is to supplement the existing requirement for access control by adding the requirement for positive personal identity. At a minimum this would eliminate the lost card vulnerability and could be integrated into a more comprehensive system for controlling employees. All employees must be enrolled in the biometric system as a condition of employment. A general procedure would entail:

- Enrollment of individuals into the system (check identity against TOWL database, and store data on a card or in a database).
- Positive verification of employee (compared against data stored on a card or database) at entrances to secure areas.
- Verification algorithm interconnected with door/gate/turnstile blocking entry.

- Door/gate/turnstile opening to allow authorized individual access.
- Provision for handling any false rejections.

2.1.2 Issues

There are many issues associated with either identifying a concept of operations or recommending the use of biometrics in an aviation environment. The issues can be categorized into three broad areas:

1. Insufficient evaluations (Technical, Scenario, and Evaluation)[6] of the use of biometrics in an aviation environment.

2. Local control of airports versus federal control, standards, and/or mandates.

3. Relatively immature state of the art for certain biometric applications.

While some studies have been conducted by respected organizations within the United States and in the United Kingdom, their use in a nationwide approach within the United States and its unique method of airport cognizance largely driven by local airport authorities poses difficulties in the deployment of such technology without policy and funding changes. Standards become very important in this context. Without a set of technical and operational standards for all biometrics under consideration (i.e., fingerprint, iris recognition, hand geometry, facial recognition), the potential exists for varying error rates, system maintenance and operation costs, and increases the likelihood of system failures. These are issues that arise in all four Focus Groups and is explained in the following subsections.

2.1.2.1 Insufficient Evaluations (Technical, Scenario, and Evaluation) of the Use of Biometrics in an Aviation Environment.

Besides funding, the biggest obstacle in evaluating technologies with numerous applications was the evaluation methodology. Until recently, no set methodology has existed that would provide results that would be useful for different applications of the same technology. A new methodology to perform these evaluations has been developed[7,8] and successfully demonstrated[9]. This methodology contains several ideals and a three-step evaluation plan that is necessary to perform prior to any pilot demonstrations.

---

6 See Evaluating Biometrics for Airport Security - An Overview by D.M. Blackburn. Available as a corollary document at http:/www.biometricscatalog.org/asbwg.

7 P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki. An Introduction to Evaluating Biometric Systems. *IEEE Computer*, Vol 33, No. 2, February, 2000, pg. 56-63.

8 D.M. Blackburn. "Evaluating Technology - Three Easy Steps to Success". *Corrections Today*, July 2001.

9 D. Blackburn, M. Bone, and P. J. Phillips. "Facial Recognition Vendor Test 2000 Evaluation Report." February, 2001. Available on the internet at: http://www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.htm.

The FAA should expect several immediate in-situ demonstrations from several different sources, many of which will produce valuable "lessons learned". These lessons learned will not be totally sufficient for determining national implementations without simultaneous technology evaluations.

Previous pilot programs can also provide valuable "lessons learned". For example, a four-year study was conducted on behalf of the FAA by Volpe National Transportation System Center (Universal Access System Program report of October 21, 1997). The integration of biometrics into the system was not addressed. The extensive effort put forth by the UAS Program offers valuable insight into the operational concerns and its recommendations and lessons learned should be taken into account before establishing any pilot program or testbed recommended by the Steering Committee. Other useful studies and standards have been established and examined by CESG[10] within the UK. Of particular interest is their series on Best Practices in biometric product testing.

Although the FAA will need to start performing several immediate in-situ demonstrations for political reasons, as well as for valuable "lessons learned", the demonstrations by themselves will not be totally sufficient for determining national implementations. A thorough technical analysis followed by scenario evaluations, which could use the systems from the in-situ demonstrations, will be required for a full understanding of system and architecture capabilities.

2.1.2.2 Local Control of Airports Versus Federal Control, Standards, and/or Mandates.

A central policy issue that will dictate the effectiveness of any program for the use of biometrics in aviation security involves local versus federal control of airports. To that end, before any firm recommendations can be made with respect to biometrics for employee access, a firm policy needs to be in place that addresses this issue. With local control of the security systems there is a risk of aircrews having to adapt to multiple systems and continue to carry multiple cards. With a federally mandated system with standards to back it up, the systems would have more likelihood of success, stability, and less cost due to economies of scale. GSA has had success in establishing its "Smart Card" program, and integration of biometrics into such a program may prove beneficial for airport security.

2.1.2.3 Relatively Immature State of the Art for Certain Biometric Applications

Some biometrics applications have not been proven and are not currently in a robust system configuration to meet the goals set forth for employee access concerns. Because of this, there will continue to be a requirement for further study and system development, operational

10 http://www.cesg.gov.uk/biometrics.

evaluation, and laboratory testing to advance the state of the art and increase system confidence.

Layering of biometrics would provide for a more robust system and should be considered. Layering is the use of more than one biometric device as part of a system solution. Layering can take two forms. The basic concept is to use a secondary biometric technology to allow automated resolution of a "false reject" based on the primary technology. Also, to thwart attempts to exploit possible vulnerabilities in biometrics technologies, the primary/secondary relationship could be randomly changed. Also, the second form of layering could be applied during periods of heightened security alert. In this case both technologies would be employed to verify identity (higher security at the expense of increased false rejections). The thought of layering biometrics is still very new and its integration has not been standardized.

2.1.3 Steering Committee Recommendation

The Steering Committee does not foresee any technological or other concerns that could keep this approach from being implemented beyond logistics issues (network installation and operational standards development). This approach also addresses the threats and goals outlined in section 1.1.1. The Steering Committee therefore recommends that the FAA should begin planning for the implementation of this approach, or similar, should funding become available.

2.2 Protection of Public Areas In and Around Airports with Surveillance.

Face recognition, as well as a few other biometric technologies currently under development, shows significant potential for combating terrorism via general or controlled surveillance. A face recognition database can serve as the investigator's memory repository of what terrorists look like. It is well accepted that humans are limited in their ability to recognize individuals that they are not familiar with. In fact, an individual under stress does not reliably recognize familiar faces in unfamiliar contexts. It is also understood that the limits of human attention (vigilance) are such that reliable detection of targets diminishes over extended time periods. Face recognition can also make investigators more efficient by automatically processing the bulk of passengers without significant human intervention. Finally, the use of face recognition would help eliminate the negative aspects of current surveillance techniques, particularly racial profiling.

2.2.1 Concept of Operations

Currently, face recognition technology is not sufficiently mature for it to be relied upon for wide area surveillance or as the sole component of an airport access control system. The technology can be used today in controlled surveillance scenarios as a security tool that can assist in

detecting terrorists on a watch list 30-90% of the time. System performance, as measured by identification and false alarm rates, depends on the method and placement of the technology.

2.2.1.1 Face Surveillance Deployment

Face recognition technology is best deployed in controlled locations that optimize system performance. Controlled locations are sometimes called "face traps". Natural chokepoints are examples of potential locations for face traps. At airports, chokepoints occur where people (passengers, airport staff, aircraft crews, and others) must slow down, line up, face and move in a known direction. These include check-in areas, security screening areas, escalators, walkways, and entrances to loading bridges used for boarding and deplanement.

2.2.1.2 Deployment Factors

Lighting. Face recognition system capabilities are significantly degraded under poor lighting conditions. Best performance results come with direct illumination onto the face of the subject from one or multiple light sources, and minimal background lighting. It is very likely that these lighting conditions will have to be created or at least controlled at selected "Face Traps" in airport environments to ensure good performance of the face recognition system.

Subject Pose. Face recognition capabilities are extremely dependent upon the pose of the subject to the face collection sensor. Best results demand a frontal view of the subject, with little variation in the tilt of the head or the turning of the head from one side to the other. Performance degrades with major subject pose variations. Multiple sensors, pointed at a subject at different angles, can be employed to mitigate the performance effects variations in subject pose.

2.2.2 Issues

2.2.2.1 Technical Issues

The quality of the face database used in a face recognition system is very important. If the images in the database are poor, then the performance of the face recognition will be degraded. The size of the watch list affects overall system performance. As the size of the watch list increases, performance decreases. A small watch list with high value terrorists will have better performance than a watch list of tens of thousands of criminals who would not be suspected of hijacking a plane.

2.2.2.2 Other Issues

The success or failure of face recognition technology employed in an airport surveillance system

will rest upon the manner in which false alarms are managed.

False Alarm Thresholds. Airport security operations personnel must understand that face recognition systems will inevitably generate false alarms. Planning for false alarm occurrence and establishing acceptable false alarm thresholds should be addressed prior to deployment of a face recognition system. Depending upon the nature of the airport security system, combined with the expected role of a face recognition capability within that system, security operators may want to consider what types of false alarm thresholds can be tolerated for a given threat environment.

Managing False Alarms. Effectively managing false alarms, in periods of decreased and increased threat postures, is important to the acceptance of the use of biometrics as a security tool in airports. In the near term, security personnel will have to develop standard operating procedures (SOPs) to manage false alarms. We can look forward to increased interaction between security operators and surveillance and knowledge systems to help resolve false alarm issues in the future.

(a) Operator (Man-in-the-loop). In the near term it is expected that false alarms generated by a face recognition system will be handled by inserting security personnel into the adjudication of the false alarm. Airport security procedures will have to be developed to assess the severity of the alarm through other means (additional identification checking, questioning of the subject, investigation of the subject's behavior and intentions, etc.).

(b) System-Operator Hybrid. In the future, it may be possible to connect the occurrence of a surveillance system alarm with the automatic initiation of a series of actions to assist security operators in resolving subject uncertainty. For example, a system alarm could trigger a 'knowledge based assisted interrogation' of the subject, perhaps combined with a rapid search of the subjects past travel itinerary.

(c) System Alarm Management. In the distant future, it should be possible for a surveillance system to, once alarmed, automatically cue additional sensors to assist in the further identification of the subject, initiate a thorough background check of the subject activities since arrival at the airport, and the case of a high value target, inform the security apparatus to deny access to the individual. Development of "suspicious behavior detection" capability is also being pursued.

2.2.3 Steering Committee Recommendations

2.2.3.1 Near Term

Investigate, via Scenario and Operational Evaluations, the use of close proximity face recognition systems at chokepoints where lighting and pose can be controlled. An example location is to incorporate them into the security screening areas for passengers. The DoD Counterdrug Technology Development Program Office is currently performing scenario evaluations of two face recognition systems in a close-range generic chokepoint with operator assistance and simple measurements akin to historical verification and identification measures. DARPA's HumanID program is also currently performing a scenario evaluation of a prototype long-range automated surveillance system using newly developed surveillance measurements[11]. These two agencies have expressed interest in jointly providing technical guidance to the FAA should the FAA deem these Scenario Evaluations successful and would want to perform an Operational Evaluation[12].

2.2.3.2 Intermediate Term

Incorporate face recognition into a comprehensive airport security system to screen passengers at chokepoints as a backup for an Aviation Security Identity Recognition (ASIR) card (see section 2.3). Incorporating the face recognition surveillance component with the ASIR function will reduce the number of false alarms, increase the number of components that a future hijacker will have to pass, and allow the incorporation of additional information into the decision making process. The inclusion of additional information will be possible because it will screen passengers before their arrival at the airport or during transit between checkpoints at an airport. Checkpoints include initial check in, security screening, and gate checking. This information includes additional biometrics and collateral information such as flight profiles and criminal records. Future biometric based surveillance systems will possess improved technical capabilities to include increased range of detection and identification, increased tolerance to poor lighting and variations in pose, and some form of sensor connectivity to ensure good image production. (These same advances can also be applied to other areas.) Future surveillance systems could extend operations to include concurrent searches of multiple images from a crowd or at airport perimeters.

2.3 Passenger Protection and Identity Verification

This area is an analysis of the efficacy of using biometrics to positively recognize the identity of all passengers who board an aircraft. This potential application is very complex and controversial because of high volume and privacy concerns. The concept calls for enrolling passengers in an Aviation Security Identity Recognition (ASIR) program.

2.3.1 Concept of Operations

11 See Appendix A.

12 DoD Counterdrug Technology Development Program Office and DARPA have a history of cooperating to evaluate and advance face recognition and surveillance technology.

The basis of a passenger recognition system is the use of an identity card with the capability of storing digital information about each passenger at some location. A description of each phase of the operation of the Aviation Security Identity Recognition (ASIR) system is described in this chapter. The focus is on a mandatory system that provides the maximum security benefit.

2.3.1.1 Enrollment

All airline passengers will obtain or purchase an Aviation Security Identity Recognition (ASIR) card at a nearby airport (or U.S. Embassies for foreigners) wishing to fly into/within the United States. Applying for an ASIR card will be similar to applying for a passport. The procedures for enrollment must include background investigations as any terrorist with an ASIR card can legitimately use it to fly in the United States. The Steering Committee must also mention that only a minority of the terrorists in the 11 September 2001 attacks were on watch lists, and could have been approved for ASIR cards, so the enrollment process must be designed with high security.

2.3.1.2 Operation

Biometric verification should be implemented at each point within a normal airline journey, where today we see manual interventions. Manning should be necessary only in the most sensitive areas. Automated systems such as access control gates or turnstiles that allow continuation only upon successful completion of the automated recognition, using the three strikes rule[13], have proven feasible in a wide range of current applications. Some level of physical oversight will likely be required to ensure that individuals do not circumvent those control barriers. However, posting an agent or guard to monitor several control gates can satisfy this requirement.

2.3.1.2.1 Ticket Purchase

Ticket purchases for airline travel would be saved to a passenger's name, as is currently done within the airline Passenger Name Record (PNR) reservation system. An added field would be placed for the ASIR number in the PNR system.

2.3.1.2.2 Check-in/Ticketing

As part of the check-in/ticketing process at either a ticketing counter or e-ticket kiosk, passengers will be asked to present their ASIR card to the attendant/kiosk. As part of the check-

13 The verification procedure would use a "three strikes" rule where it would require three successive negative verifications before the passenger would be directed to a secondary process similar to current procedures using metal detectors.

in process, a live capture of the passenger's biometric would be compared against that contained on the card, or within the ASIR system database. Once the passenger's identity has been verified and security questions have been answered correctly, the check-in process could continue and boarding passes for the flights in question issued. Conceivably, boarding pass and checked baggage information could be saved to the card as an additional security control feature.

If the ASIR system is voluntary, ticketing could also occur at the gate. Automated kiosk check-in should be prohibited without proper identity verification using biometrics.

2.3.1.2.3 Security Checkpoint

Passing through the security checkpoint could be done using automated optical turnstiles with biometric verification (using information stored on the card or a national database). Ideally, this process should be fully automated wherever full biometric scanning and comparison capabilities are implemented. Manual intervention should normally occur only in those situations where automated identity verification cannot be accomplished. Inclusion of retrievable boarding pass information on the card will facilitate this step to a great extent.

If the ASIR system is voluntary, a security officer would manually compare their identification (e.g. driver's license) and boarding passes to allow entrance through the checkpoint.

2.3.1.2.4 Boarding

As part of the boarding process, passengers will gain entitlement to board the aircraft by initiating an automated identity verification process by use of the ASIR card. Some believe additional identity verification is required at this point, while others believe it to be an unnecessary step if previous positive verification has occurred.

If ASIR is a voluntary system, security personnel would be required to allow individuals without ASIR to board only after a successful interview and manual identity verification.

2.3.1.2.5 Customs and Immigration

Persons entering the United States from overseas must pass through an immigration checkpoint at the port of entry. At this checkpoint, an INS official scrutinizes the person and inspects his or her travel documents. The official then makes a decision as to whether the person may enter the United States. This immigration checkpoint is one of the nation's vital first lines of defense against a terrorist entering the country. From the perspective of counter-terrorism, this checkpoint is a chokepoint where a foreign terrorist is most vulnerable. This is the first and likely only place in the U.S. where trained federal officials will closely scrutinize them. Individuals in possession of an ASIR card could be allowed to proceed rapidly through this process through a system such as the existing INSPASS system.

2.3.1.2.6 Re-enrollment.

Studies have shown that a time difference between the enrolled biometric signature and a present biometric signature adversely effects performance of many biometric systems. Periodic re-enrollment would therefore make the system more accurate, thus making the passengers happier. Re-enrollment could be done via a kiosk for the biometric signatures stored on the card or at special counters for the national system. It may also be possible for some biometric devices to update the stored biometric signatures based on information made available through using the system (i.e. a dynamic template).

2.3.2 Issues

2.3.2.1 Technical Issues

The type of biometric, or vendor, most suited for this application cannot be absolutely determined at this point because of the absence of government-run Technology Evaluations. The most mature systems for this application are hand geometry and fingerprint. Iris recognition is emerging as a high accuracy alternative (with some possible drawback in terms of cost, throughput, and user acceptance).

Network and card protocols would need to be developed for this application. Network failure could ground flights at a specific airport, region or nationally. (See Chapter 3 for more discussion on this issue).

Standards for biometric devices are not universally accepted.

Implementation of this application would be extremely difficult due to coordination issues between the government, air carriers and individual airports. The cost for this application would be significant.

2.3.2.2 Other Issues

Some suggestions have been made to link existing travel documents (travel documents, drivers' licenses, frequent flier cards, passports, visas, INSPASS, CanPass, Interagency Border Inspection System by US Customs, etc.) to quickly develop a passenger identity verification system. The Steering Committee believes that this approach would take as much, if not more, time and effort to develop than a new system but would also leave the security system open to more holes than a newly designed system. There is no realistic possibility for a "quick" implementation for passenger identity verification. The FAA will not be able to solve this problem on either a US or global scale overnight, and should therefore beware of being too

prescriptive at this point.

Given the number of non-citizens on domestic flights, there may be strong limitations on the FAA's authority to mandate specialized passenger recognition systems for all US and US-bound air traffic. A mandated system would provide the greatest impact on deterring or defeating terrorism, but would also meet with a large fight from civil libertarians. Much thought has also been given to a "two-tier" system consisting of volunteers and remaining passengers. Proponents of this approach comment that it makes sense if we want to allow those that we know are non-threats to proceed rapidly, thus allowing security to focus their screening resources on unknown travelers. The security of this two-tiered system would be very limiting, as terrorist would simply decline to participate, or look for vulnerabilities in the two-tiered system. If the two-tiered system is done incorrectly, passengers may start to feel that it is not as secure. For example, it does no good for one individual to voluntarily pay for some extra security measure if the individual behind them simply walks through as usual and straight onto the plane.

Should security systems be database centered or individual location centered? Both approaches have advantages and disadvantages. A database-centered approach (either national, regional, or airport) would require a vast security network for its operation. A national database-centered approach would permit the usage of proximity, mag-stripe, or other 'dumb' card, which some believe has higher security because there is no way any identity information could be derived solely from the card.

Smart cards could be used for the "individual location centered" approach, where all of the biometric information is stored on the card and is retained by the individual. Smart cards could also be used for the national system, and would be required for regional or airport systems. The 'dumb' card approach would receive the most criticism from privacy advocates because of the potential for data analysis on travel patterns of the general public. The 'smart' card approach has greater potential for fraud and would not allow the government to automatically revoke a card.

This application would generate significant issues for the flying public. These include privacy concerns as well as passenger training on how to use the new system.

2.3.3 Steering Committee Recommendation

From a completely personal standpoint, no one on the Steering Committee wants to mandate an ASIR program. Cost, implementation, and privacy issues strongly suggest that this approach should not be high on the priority list for aviation security. However, the implementation of this approach has the highest potential for deterring and stopping terrorists from using the aviation industry for further attacks. The Steering Committee's opinion is that they are not the proper individuals to recommend or not recommend this application for implementation. Congress can only make a decision of this magnitude.

2.4 Aircrew Identity Verification (Ground and In-Route).

Biometrics can be incorporated into aircrew and ATC operations in much the same way as the systems described in section 2.1 and 2.3 to reduce potential threats.

2.4.1 Concept of Operations

2.4.1.1 Pre-Flight Aircrew Verification

Crew identities need to be positively verified through the combination of two biometrics at the Airline Flight Operations Center. Of all of the biometrics available, the Steering Committee believes that iris and fingerprint could be the technologies with the greatest potential, but Technology Evaluations must be performed to analyze this assumption. Alternatively, speaker recognition could be used instead of fingerprints as this biometric will also play a significant role in later in-flight identity verification. The combination of two biometrics should significantly minimize any chance of false identification.

At the same time, crew identities can be cross-referenced to other legitimate crew members that will be on the plane, validated by FAA or airline database, downloaded to the aircraft directly or into air crew "smart cards," and transmitted to air traffic control for in-flight verification/identification. Information that should be downloaded would include as a minimum:

- Identification information cross-referencing assigned members of the flight crew or air marshals for this specific flight.
- Identification information on the specific aircraft being utilized for the specific flight.
- A time stamp of when verification occurred in the Flight Lounge

2.4.1.2 Onboard Re-verification

Crew identities should be re-verified upon boarding their aircraft by presentation of a single biometric and their smart card. The system should verify that all crew have checked in and monitor the amount of time between initial verification and aircraft check-in for discrepancies. The focus group believes that fingerprint is most suitable for this application. The fingerprint system should be interconnected with the aircraft control system and its results should be both logged onboard the aircraft and transmitted to ATC.

2.4.1.2 In-flight Re-verification

In-flight re-verification of identities should occur between air traffic control and the aircrew. This should be incorporated covertly in standard air traffic control communications and overtly

in the event of an alarm condition on-board the aircraft. Speaker recognition was most recommended and the U.S. Air Force has a significant amount of experience in its use. Face recognition is also a technical possibility, but is not being recommended by the Steering Committee because of anticipated resistance by pilot unions. Speaker verification can be performed locally in the aircraft as well as remotely at the ATC, although local verification will allow much higher quality sound input prior to transmission.

Re-verification should also be triggered in-flight by intelligent monitoring of aircraft "health" by on-board and ATC systems. NASA already provides sophisticated onboard and ground-based "health" monitoring systems that make alarm situation determinations indirectly by overseeing the actions and behaviors of the crew and the state of the aircraft. Today's high-end aircraft engines are already providing in-flight performance monitoring and transmission to ground-monitoring systems and there may be a possibility to take advantage of systems like this for further status monitoring.

2.4.1.3 Identification of Pilot Takeover

The Steering Committee determined that there is not a major need to attempt identification of an individual that takes over control of the airplane in-flight, as all takeovers are considered equally hostile. The Steering Committee believes this should only be done if biometric devices installed for application 2.4.1.2 could be used for this as well. It should be noted that biometrics can only identify individuals which have a biometric template stored on file in a database. Most of the recommended technologies for this application only support voluntary capture and storage of biometric templates.

2.4.2 Issues

2.4.2.1 Technical Issues

The type of biometric, or vendor, most suited for the applications described in sections 2.4.1.1 and 2.4.1.2 cannot be absolutely determined at this point because of the absence of government-run Technology Evaluations. However, technology category recommendations have been expressed.

The application in section 2.4.1.1 requires communication between the Operations Center and aircraft. The applications described in all sections require integration of new technology into the aircraft.

2.4.2.2 Other Issues

Cooperation with pilots unions, air carriers and individual airport authorities will be required.

2.4.3 Steering Committee Recommendation

The Steering Committee does not foresee any technological or other concerns that could keep this approach from being implemented beyond logistics issues (network installation and operational standards development). The Steering Committee recommends that aircrew identifications be verified during pre-flight operations planning, on the aircraft prior to takeoff, and in-flight as part of standard operations. This approach also addresses the threats and goals outlined in section 1.1.4. The Steering Committee therefore recommends that the FAA to should begin planning for the implementation of this approach, or similar, should funding become available.

3. 0 Overall Issues

3.1 Biometric Standards

Interoperability of biometric devices is a critical consideration for these applications if the FAA decides to allow using different types of biometrics at different locations. Even if a specific biometric type and vendor are chosen, standards must be in place to facilitate the integration of future improved biometric technologies. Unfortunately, these standards do not exist to facilitate this interoperability.

One group, the BioAPI Consortium[14] is attempting to develop industry-wide standards that would solve this problem. The BioAPI Consortium is a group of over 50 organizations that have a common interest in promoting the growth of the biometrics market. BioAPI is dedicated to developing a specification for a standardized Application Programming Interface (API) that will be compatible with a wide range of biometric applications programs and a broad spectrum of biometrics technologies. The API description defines how application programmers and biometric solution vendors write to the common BioAPI interface. If successful, the BioAPI runtime framework will allow applications to interoperate with various biometric solutions.

Version 1.0 of the BioAPI specification was published in March 2000. It is the intention of the BioAPI consortium to submit its completed specification for adoption by a recognized standards group. A liaison committee for interface with external standards groups has been formed, chaired by Fernando Podio of NIST, who is also co-chair of the Biometric Consortium. The committee will investigate the various avenues for standardization and recommend a standardization plan to the BioAPI Consortium. Although much work has gone into the development of the BioAPI specification, the work that remains is daunting: community acceptance, adoption by a recognized standards group, establishing a test program to ensure compliance, and finally

14 http://www.bioapi.org.

BioAPI-approved biometric solutions.

3.2 Database

There are many unknowns concerning the content and distribution of biometric databases to support aviation security operations: Should there be separate databases for each application? Who should be in the database(s)? What agencies, or possibly governments, should have access to the database(s), and which should be tasked with their responsibility? Who would have oversight? Should the database(s) be maintained on local machines, on airport servers, or a national server? How do you update the database(s) securely? These questions, while outside the scope of this working group, need to be answered before wide scale implementation of biometric systems across the aviation industry. Solving these issues could fall within the charter of the newly established Office of Homeland Security.

3.3 Privacy

Current legal standards recognize that we are all subject to heightened scrutiny at our borders and ports of entry. The "border exception" to the Fourth Amendment recognizes "the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." Accordingly, such searches are reasonable and do not require a warrant, probable cause, or even reasonable suspicion. When we transit our borders, therefore, the authorities can closely scrutinize our person and property in ways that they could not do in another setting. Even within our own borders, the law requires airport facilities to conduct security screening of passengers' persons and personal effects, and it is unlawful even to make jokes about threats on airport property.

Many states have legislation that prevents electronically encoding any data on an official document that cannot be visually verified by the owner of that data. Most also have restrictions on the electronic collection and transmission of personal data without the express permission of the owner. Further, many states strictly prohibit the use of personal data for any purpose other than that for which it was originally collected – and nearly all strictly control or prohibit archiving of that data.

Legalisms aside, biometric technology is still relatively new for the majority of U.S. citizens. This unfamiliarity leads to several concerns, even when used in a legal and ethical manner. The simple fact that a passenger has a concern makes it necessary that the FAA works to alleviate these concerns. These issues can be divided into three different types: physical, religious and informational[15].

Physical. A large percentage of our population associates a fingerprint with felons, and

15 Woodward, Webb, Newton, Bradley, and Rubenson name the three categories of concerns in "Army Biometric Applications". Published by RAND in 2001

feels cheapened if requested (or required) to submit a fingerprint. Retinal scanning devices have suffered for years because of the perception of harm due to the 'laser in the eye' myth. Finally, any type of biometric device requiring someone to touch a sensor that others have touched (fingerprint and hand geometry for example) can cause concern for some individuals because they consider it unhygienic, even though they may routinely touch doorknobs and computer keyboards.

Religious. Religious concerns about the use of biometrics could arise from a variety of different groups. An all-inclusive analysis of religions and their views on the use of biometric technologies is beyond the scope of this paper and the working group. However, analysis of potential religious concerns before installation of an application using biometrics is suggested.

Informational. Many of the concerns in news articles related to the face recognition installations at the Super Bowl or in Ybor City are caused from incorrectly confusing a technology (face recognition) with applications of a technology. Biometric technologies by themselves are only capable of developing and comparing matrices to each other and producing a similarity score. Applications that use biometrics can cause enormous concern for individuals because of the possibility of eventually using data for applications other than what was first envisioned. This is referred to as "function creep" and could be both positive (finding parents delinquent in child support payments) and negative (selling DMV photos to a commercial firm).

To alleviate many of the concerns being expressed in the U.S. and overseas, primarily by European governments, we will need to see a global agreement on data control and collection. Further, travelers, who actually own the data, will need to be educated about the benefits to be accrued through provision of such data voluntarily. Benefits to the traveler beyond heightened security are suggested[16].

3.4 Selection of Biometric Technologies

Previous sections have shown the need to have technology evaluations of potential biometric technology followed by short scenario evaluations. Performing an evaluation that follows proper ideals and procedures, such as the Facial Recognition Vendor Test 2000, will ensure that the FAA chooses the proper biometric type and vendor. Making this decision without proper evaluations would amount to educated guessing, which is not acceptable for this important endeavor. An R&D cycle may be necessary to improve the technology, but that cannot be determined before receipt of evaluation results.

3.5 Ongoing demonstrations

16 Appendix G - Non-Security Related Benefits

Numerous airports have individually announced that they have planned to demonstrate/evaluate some form of biometric technology for numerous different applications. The vast majority of these demonstrations have not been coordinated with the FAA. If done properly, the results from these demonstrations/evaluations could be beneficial. If done improperly, the results will be detrimental. In either case, these evaluations add another issue, as any federal implementation of biometric technology would need to integrate and/or replace the systems previously put in place.

4. Conclusions

The purpose of the Aviation Security Biometrics Working Group was to bring together representatives of Federal Agencies, combined with information gathered from government, industry, and academia, to develop an overview of the technological, operational, and political issues associated with incorporating biometric technology into aviation security for submission to the Federal Aviation Administration.

The Working Group studied the efficacy of incorporating biometric technology into aviation security. Within the aviation security realm, four distinct application opportunities were described.

1. Employee identity verification and access authorization.
2. Protection of public areas in and around airports using surveillance.
3. Passenger protection and identity verification.
4. Aircrew identity verification (ground and in-route).

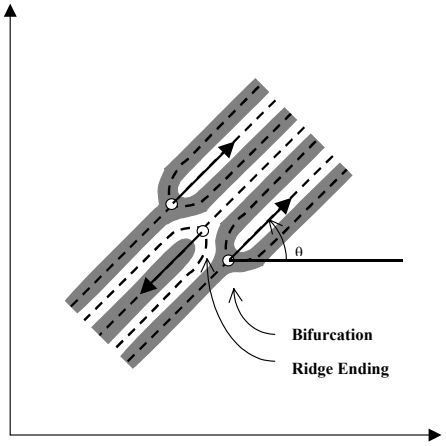
This paper has shown that the use of biometrics in each of these areas would significantly contribute to aviation security systems. The exact extent of this contribution, and in some cases the biometric type and vendor, cannot be determined at present for most application opportunities because of the lack of formal government Technical, Scenario, and Operational evaluations. In order to add biometric technology to aviation security in the near future, these evaluations and the finalization of standards activities must be performed.

Appendix A – Biometrics

A.1. Biometric Type Description[17]

A.1.1 Fingerprint

The fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves a user placing his finger on a platen for the fingerprint to be read. The minutiae are then extracted by the vendor's particular algorithm to create a template. Fingerprint biometrics have three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) for law enforcement uses, fraud prevention in entitlement programs, and access control for facilities or computers.



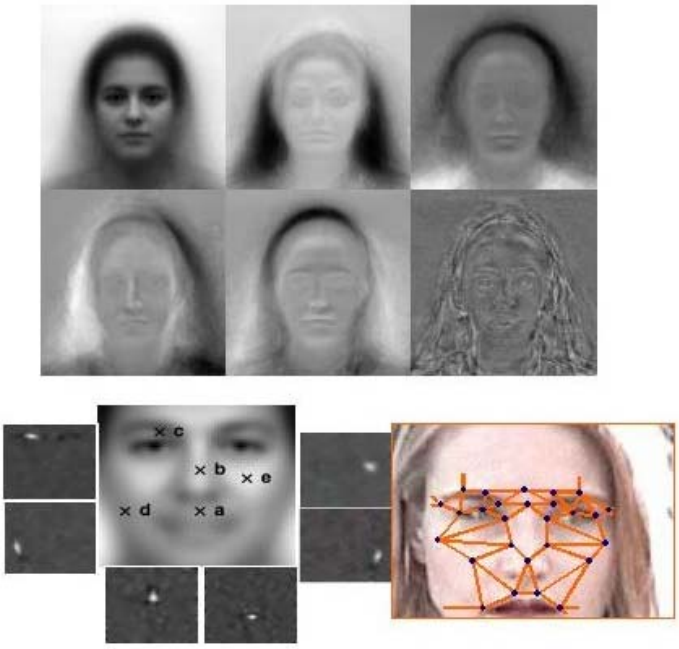
A.1.2 Hand Geometry

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods takes prints of the palm or fingers. Rather, only the spatial geometry is examined as the user lays his hand on the sensor's surface and uses guiding poles between the fingers to place the hand properly and initiate the reading. Finger geometry typically uses two or three fingers. During the 1996 Summer Olympics, hand geometry secured access to the athletes' dorms at Georgia Tech. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users.

17 Text descriptions of biometric types in Appendix A taken from "Army Biometric Applications – Identifying and Addressing Sociocultural Concerns" by Woodward, Webb, Newton, Bradley, and Rubenson, RAND.

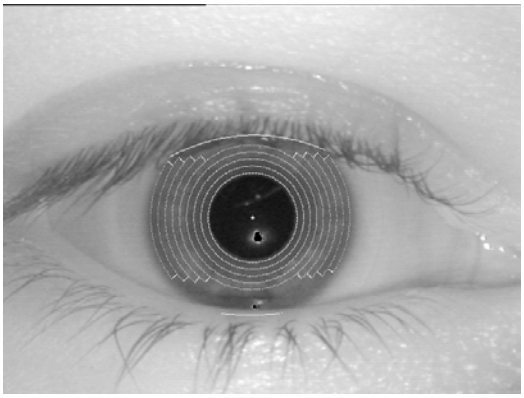
A.1.3 Face Recognition

Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. Different methods of facial recognition among various vendors all focus on measures of key features. Noncooperative behavior by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies. Facial recognition has been used in projects designed to identify card counters in casinos, shoplifters in stores, criminals in targeted urban areas, and terrorists overseas.



A.1.4 Iris Recognition

Iris recognition measures the iris pattern in the colored part of the eye (although the color has nothing to do with the scan). Iris patterns are formed randomly. This means no two iris patterns are the same; the iris pattern of one's left eye is different from the iris pattern of the right eye. Iris scans can be used for both identification and verification applications. ATMs ("Eye-TMs"), grocery stores (for checking out), and the Charlotte/Douglas International Airport (physical access) use iris recognition in test applications. During the 1998 Winter Olympic Games in Nagano, Japan, an iris recognition identification system controlled access to the rifles used in the biathlon.



A.1.5 Speaker Recognition

Speaker Recognition is an automated method of using vocal characteristics to identify individuals using a pass-phrase. The technology itself is not well developed, partly because background noise affects its performance. Additionally, it is unclear whether the technologies actually recognize the voice or just the pronunciation of the pass phrase (password) used to identify the user. The telecommunications industry and the National Security Agency (NSA) continue to work to improve voice recognition reliability. A telephone or microphone can serve as a sensor, which makes this a relatively cheap and easily deployable technology.

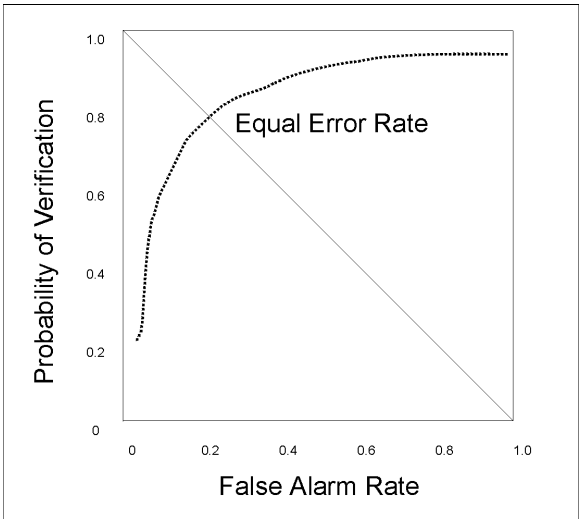
A.2 Performance Measures[18]

Biometric developers and vendors will, in many cases, quote a false acceptance rate (sometimes referred to as the false alarm rate) and a false reject rate. A false acceptance (or alarm) rate (FAR) is the percentage of imposters (an imposter may be trying to defeat the system or may

18 Some text in section A.2 is taken from the Facial Recognition Vendor Test 2000 Evaluation Report by Blackburn, Phillips, and Bone. http://www.dodcounterdrug.com/facialrecognition

inadvertently be an imposter) wrongly matched. A false rejection rate (FRR) is the percentage of valid users wrongly rejected. In most cases, the numbers quoted are quite extraordinary.

The false acceptance rate and false rejection rate are not mutually exclusive. Instead, there is a give-take relationship. The system parameters can be changed to receive a lower false acceptance rate, but this also raises the false rejection rate and vice versa. A plot of numerous false acceptance rate-false rejection rate combinations is called a receiver operator characteristic curve. A generic ROC curve is shown below. The probability of verification on the y-axis ranges from zero to one and is equal to one minus the false reject rate. The false acceptance (or alarm) rate and the false reject rate quoted by the vendors could fall anywhere on this curve and are not necessarily each other's accompanying rate. Some spec sheets also list an equal error rate (EER). This is simply the location on the curve where the false acceptance rate and the false reject rate are equal. A low EER can indicate better performance if one wants to keep the FAR equal to the FRR, but many applications naturally prefer a FAR/FRR combination that is closer to the end points of the ROC curve.

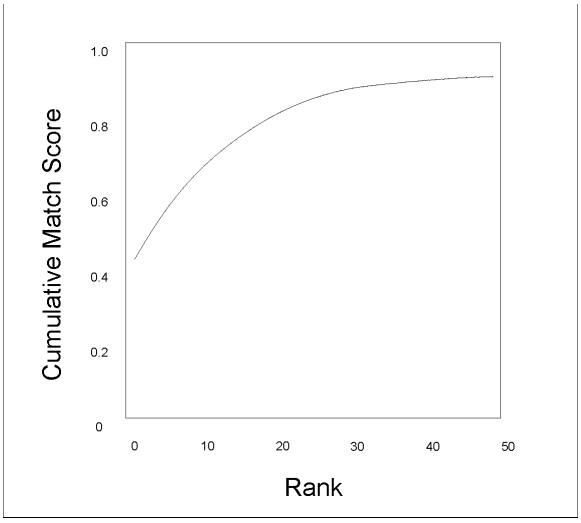


It is extremely important to note that this curve varies on the biometric type, choice of vendor, and application setup. It is impossible to obtain an understanding of system capabilities by looking at an ROC curve unless one knows what data was used to make these curves. An ROC curve for a fingerprint system that obtained data from coal miners would be significantly different from one that obtained data from office workers. Other biometrics will also vary depending on the setup and user activity.

The above description is valid for displaying verification results. In a verification application, a user claims an identity and provides their biometric. The biometric system compares the biometric template (the digital representation of the user's distinct biometric characteristics) with the user's stored (upon previous enrollment) template and gives a match or no-match decision. Biometric systems can also act in an identification mode, where a user does not claim an identity but only provides their biometric. The biometric system then compares this biometric template with all of the stored templates in the database and produces a similarity score for each of the

stored templates. The template with the best similarity score is the system's best guess at who this person is. The score for this template is known as the top match.

It is unrealistic to assume that a biometric system can determine the exact identity of an individual out of a large database. The system's chances of returning the correct result increases if it is allowed to return the best two similarity scores, and increased even more if it is allowed to return the best three similarity scores. A plot of probabilities of correct match versus the number of best similarity scores is called a cumulative match characteristics curve. A generic CMC curve is shown below.



Just as with ROC curves, these results can vary wildly based on the data that was used by the biometric system.

Identification has been historically viewed as a one-to-many search against large databases where a human investigator views the search results. Such functionality is usually utilized "off-line" for investigative or intelligence purposes. Surveillance is also a one-to-many (video input with selected/developed single image sent for comparison) comparison where an investigator only views the results if any of the similarity scores are above preset threshold. This application has false alarms similar to verification, but also the ranking issues of identification. Measurables for surveillance are currently being developed as part of DARPA's HumanID program.

Appendix B – Card Technology

B.1. Technology Overview

Card types commonly used for access control can be divided into 'dumb' cards and 'smart' cards. Dumb cards are the less expensive of the two and, because they perform only one function, they are the simplest to add to an access control system. Smart cards are more powerful, and therefore more complex and costly than dumb cards. They offer many security safeguards not found in other card technologies.

B.1.1 Dumb Cards

Magnetic stripe (mag stripe) cards are the most prevalent in an individual's every day use. Most credit cards utilize magnetic stripe technology. These cards are also extensively used in security applications because of their low cost.

Prox cards contain a wire loop antenna capable of communicating with a reader using a radio frequency (RF) field. Unlike contactless smart cards (discussed below), prox cards are only capable of sending an ID number to the reader. The card manufacturer sets the ID number during production and assures that it is unique. Since the card does not store any personal information about the user, a database must be connected to the reader in order to match the ID number with the user and make access decisions. For this reason, prox cards are typically used in a networked, rather than standalone, configuration.

B.1.2 Smart Cards

The basic components of a smart card are similar to those of a computer. They are listed below:

CPU - The "brain" of the card is the CPU, which executes the instructions that give the card its calculating power.

ROM - The card also has Read Only Memory (ROM), which stores fixed data, such as the card operating system, and the program or application memory, or the instructions that the CPU executes to perform an assigned task.

RAM - The card's Random Access Memory (RAM) temporarily stores incoming data, calculated values, or the results produced by the CPU during its operation. On a smart card, this memory functions as the card's scratchpad.

NVM - The card's Non-Volatile Memory (NVM) is analogous to a hard disk drive. It stores data that changes during the operation of the card and retains the information after

power is removed. The type of NVM memory most commonly used in smart cards is the Electrically Erasable Programmable Read Only Memory (EEPROM). This memory can be written to and read from many times.

Smart cards have growing memory capacities, as well as strong lifecycles. Smart card memory capacities are available up to 32k with 16k currently the most popular. The lifetime of most smart card memories is rated at a minimum of 1 million read/write cycles. Data can be encrypted on a timecard, and the NVM can be subdivided with different access restrictions and encryption.

There are three types of smart cards: contact cards, contactless cards, and combination cards. These three types are distinguished by how they communicate with the smart card read/write device.

B.2 Card Standards

B.2.1 Technical Standards

Physical characteristics of smart cards are specified by standards outlined by the International Standards Organization (ISO). All smart cards must conform to ISO standard 7816-1/2/3. The 7816-1 standard defines the dimensions of the card, which are the same as a standard credit card. The 7816-2 standard defines the dimensions of the card and the location for the chip interface contacts. The 7816-3 standard requires the cards to support the T=0 asynchronous communication protocol. Although only the T=0 protocol is required by ISO, some cards support both the T=0 and T=1 protocols, enabling them to interface with a greater number of card read/write devices. Characteristics of contactless smart cards are specified by ISO/IEC 14443.

Some references have listed ANSI NCITS 322 and ISO 10373-1 as standards for testing the durability of the card structure. The Focus Group was not able to analyze these standards.

B.2.2 Operational Standards

No standards exist for cards specifically for the aviation industry.

Appendix C – Card Reader

C.1. Technology Overview

Card readers, like the cards, have many features that must be considered when designing a system. To cover this variety of applications, there are many different types of readers designed for specific purposes. The choice of readers depends on the type of card being used, the location of the reader, and the computers and other devices that will be connected to the reader.

C.1.1 Card Reader Requirements

Regardless of the type of reader used for a card access control system, readers must comply with certain requirements.

C.1.1.1 Hardware Requirements

The hardware requirements for smart card readers used in access control applications involve meeting international standards, as well as meeting the needs of the applications' functionality.

C.1.1.2Installation and Operating Environment

The choice of card readers may depend in large part upon the environment in which they will be installed and used. If a reader is to be used indoors at room temperatures, one built with standard, commercial grade electronic components can be selected. For effective operation in a wider range of temperatures, between -40 F (-40 C) and 125 F (52 C), industrial grade components must be used. To accommodate even greater temperature extremes, more expensive military grade components must be used. Regardless of the location of installation, the readers will require an external power supply.

C.1.1.3Regulatory Approvals

A card reader must meet several regulatory approvals. First are the standard requirements for electronic equipment, such as Federal Communications Commission classification and Underwriters Laboratory (UL) listing. Readers integrated into a security system may face stricter requirements. Requirements that ensure that readers have a certain level of operability in case of power loss, known as life requirements, may also apply. (The life requirement can be met if the reader is powered by the access control terminal, with a corresponding battery backup.)

C.1.2 Types of Card Readers

There are several different types of card readers. These readers are distinguished by how they communicate with the card, and whether or not they can be programmed.

The first distinguishing feature of card readers is how they communicate with the smart cards. Some readers communicate with cards through electrical contacts when the cards are inserted. By making electrical contact with a card's circuitry, these contact readers provide power to drive the microprocessor of the card. On the other hand, some card readers communicate with cards through RF. Since these contactless cards must operate only on the power they can extract from an incoming radio signal, a contactless card reader must contain a radio transmitter and a receiver. Both contact and contactless readers may connect to a host computer's communication port.

C.1.3 External Communications

In addition to controlling memory and input/output devices for user interaction, all of which is considered internal, the reader program handles all external communication. External communication includes communication with the card, communication with a host system, and possibly communication with other peripheral (e.g. Biometric) devices.

When a reader is expected to operate in an on-line fashion, communication must be established with a host computer. Thus, in an access control system, an interface must be established between a programmable reader and an access control terminal. This interface usually consists of six wires between the two devices.

Besides the communications port connecting to the host computer, the programmable reader may also have a second communications port. This port can be controlled by the reader program to permit interfacing with other equipment. For example, a second communications port can be used for direct interfacing with a biometrics device.

C.2 Standards

See B.2.2

Appendix D – Analysis of Biometrics for Employee Protection - Identity Verification and Access Authorization, Passenger Protection and Identity Verification, and Biometrics for Aircrew Identity Verification (Ground and In-Route)

D.1 Enrollment

The only instance that a biometric system would operate in identification mode for these application areas is during enrollment to compare them to the biometric signatures in the Terrorist on Watch List (TOWL) database.

The proper biometric for this application is limited by the data that is in the TOWL database. Fingerprint recognition has historically been the biometric of choice for large database identification applications. The Steering Committee anticipates that this database would consist primarily of surveillance photos. Therefore, the options for biometric systems for this enrollment application must include face recognition.

Of the two, fingerprint is generally accepted as the better option for ranking large databases for a human to make final comparisons. Unfortunately, we do not have fingerprint images of most suspected terrorists so the FAA should consider using both biometrics during enrollment. The setting of thresholds is not an issue as the enrolling federal agent will look at the top 'x' scores regardless of similarity score.

The Facial Recognition Vendor Test 2000 (FRVT 2000) provides identification scores for a variety of experiments. Because of the wild variation in image quality anticipated for this application, it is impossible to predict a general accuracy of 'y'% in the top 'z' similarity scores. The FRVT 2000 does tell us that lighting, pose and temporal (time) variations between the recently acquired image and the image in the TOWL database could significantly reduce the ranking position of the correct match.

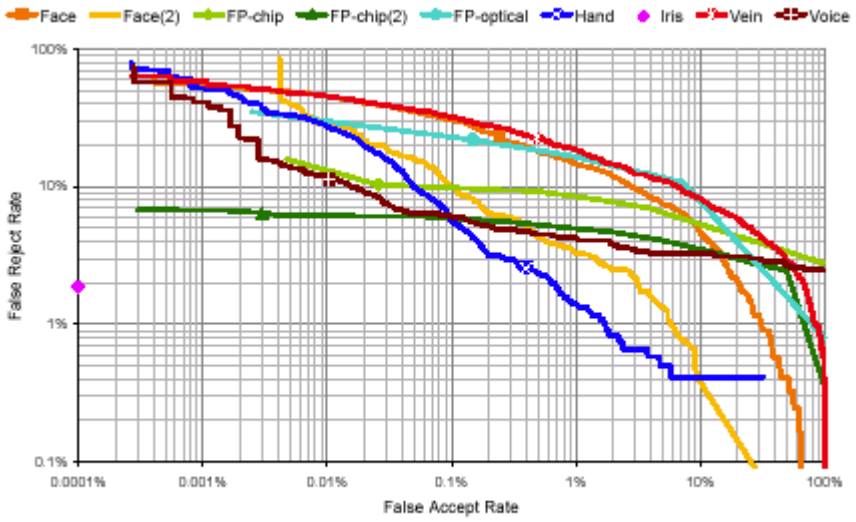
D.2 Operation

Several biometric technologies hold potential for the verification applications within these application areas. Unfortunately, in-depth Technology Evaluations that are required for the Focus Group to determine which biometric type and vendor is best do not exist for all of these technologies to be able to determine which application would be best.

The UK's Biometrics Working Group (BWG) performed a scenario evaluation that is somewhat related to these application[19]. Results from this evaluation should not be taken to be definitive for this application. Indeed, there are many potential insertion points for biometric technology for this application. The anticipated capabilities of a biometric system will vary at each insertion point.

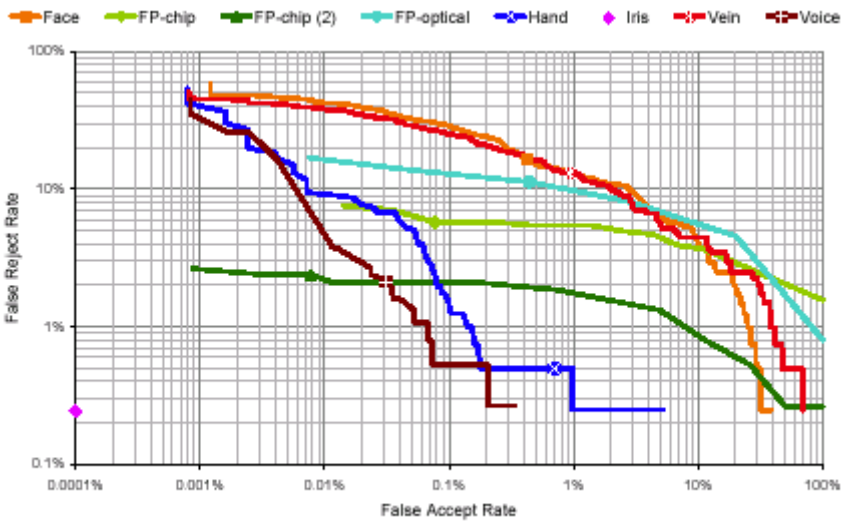
19 BWG's Biometric Product Testing Final Report by Mansfield, Kelly, Chandler, and Kane.

Even though the BWG report will not allow us to obtain an accurate estimate of performance, the results at our selected operation points vary enough to tell us that the best biometric(s) will vary by the choice of verification threshold. Also note that the BWG only tested one vendor per biometric type. Results from the Facial Recognition Vendor Test 2000 unequivocally shows that performance will vary significantly by vendor within each application and between applications. Additionally, the change in scores for a one-hit-to-secondary and a three-consecutive-hit-to-secondary vary significantly.



CESG/BWG Figure 5. Detection error trade-off: FAR vs FRR

One Strike and You're Out		
	FRR = 1%	FRR = 3%
Face	30%	15%
Face (2)	6%	1.5%
FP-Chip	Unable to reach FRR = 1%	80%
FP-Chip (2)	70%	20%
FP-Optical	80%	26%
Hand	1.7%	0.25%
Iris	Stationary 2% FRR and 0% FAR	
Vein	85%	50%
Voice	Unable to reach FRR = 1%	30%



CESG/BWG Figure 6. Detection error trade-off: Best of 3 attempts

Three Strikes and You're Out		
	FRR = 1%	FRR = 3%
Face	25%	12%
Face (2)	Not tested	
FP-Chip	Unable to reach FRR=1%	18%
FP-Chip (2)	8%	<.001%
FP-Optical	80%	30%
Hand	0.2%	.085%
Iris	Stationary 2% FRR and 0% FAR	
Vein	40%	18%
Voice	0.06%	.02%

The paper "The Psychology of Human Face Recognition" by Graham Pike (University of Westminister), Richard Kemp (University of Leichester) and Nicola Brace (U.K. Open University) gives an idea of how well humans can perform these same verification applications. This paper discussed an experiment to test the ability of trained supermarket cashiers to match shoppers to photo ID cards. A group of "shoppers" were each given four credit cards: one with a picture of the shopper taken on the same day, one with picture taken within the last 6 weeks exhibiting "minor chages" in appearance; one with a picture of a randomly chosen different shopper; one with a "matched foil", that is a picture of a shopper that looked somewhat like the card holder.

The store cashiers were aware that a test was taking place. They "accepted" 50% of all fraudulent cards as valid, 34% of the randomly assigned impostor cards were accepted as valid. 7% of the genuine same day photos were rejected and 14% of the genuine, but "aged", photos were rejected.

The study indicated that in actual practice, using cashiers who were not aware that a test was being conducted, the embarrassment and damage of false rejections would be so high that no cashier would risk such a cost. The study concludes that the actual false acceptance rate would probably be much higher in practice.

Formal technology evaluations of all appropriate biometrics must be performed, and scenario evaluations should be performed, prior to settling on a particular biometric type(s) for this application.

An in-depth technology evaluation of face recognition for verification applications can be found in the Facial Recognition Vendor Test 2000.

Appendix E – Analysis of Biometrics for Protection of Public Areas In and Around Airports with Surveillance

Surveillance is a one-to-many (video input with selected/developed single image sent for comparison) comparison where an investigator only views the results if any of the similarity scores are above preset threshold. This application has false alarms similar to verification, but also the ranking issues of identification. Measurables for surveillance are currently being developed as part of DARPA's HumanID program

Appendix F – Card Standards (Operational)

A set of operational standards will need to be developed for the cards required for the applications described in sections 2.1, 2.3, and 2.4. This operational standard, when added to the technical standard discussed in Appendix B and C, would enable multiple applications of the ASIR card as well as enable multiple vendors of cards and card readers to participate in the program. The example to follow for operational standards of cards is the American Association of Motor Vehicle Administrators (AAMVA) National Standard for the Driver License/Identification Card. The objectives of the ASIR standard should mirror the objectives of the AAMVA standard:

- Uniquely identifies the card issuer and cardholder.
- Brings uniformity to all cards in circulation.
- Encourages transition from existing practices to the new standard.
- Assists administrative efficiency and accuracy through machine-readable identification within a foundation that encourages future applications.
- Facilitates future development in technology and application.

The operational standard should, at a minimum, outline the following:

- Define the data elements
- Define the location for storage of data elements
- Define for covert and overt security (non duplication) features
- Define which data elements should be encrypted and how
- Define the physical appearance of the card
- Define expiration period of the card
- Define how airlines can mark an individual as undesirable/prohibited

Appendix G - Non-Security Related Benefits

Most passengers are amenable to increased security at our airports at the present time due to the events of 11 September, but this may change as time goes on. For long-term acceptance of the ASIR system, passengers will need to see additional benefits before they will willingly approve of the solution. There have been a few successfully implemented projects in the commercial sector using related technology that provide a significant lesson for this application: individuals tend to be less scared of a new technology if they see and understand its benefits. Examples include:

- Walt Disney World. Using mag-stripe cards and biometrics to enable season-pass holders to enter the facilities quicker.

- Washington Metropolitan Area Transit Authority. Using smart cards as an alternative "ticket" for entrance and fee payment instead of paper cards. Advantages of the smart card are quicker entrance/exit from the Metro facilities and the ability to add money to the card via credit card.

- Grocery Store VIP cards. Using mag-stripe cards as a way to provide special discounts at the time of purchase and to provide coupons based on previous purchases.

- Gas Station Quick-fill. Using proximity cards/tokens that are linked to a specific credit card to enable customers to purchase gasoline without having to wait for credit card authorization.

- Toll-lanes. Using proximity tokens linked to an account (instead of paying cash) to allow passengers quicker movement through tolls.

For passengers to welcome this new technology system, they must see some personal benefit above understanding it is contributing to their safety. The following benefits could easily be provided using the ASIR card:

Baggage claim. If a bag is lost, the flight information and baggage receipt was saved onto the ASIR card, thus making airline notification of lost luggage much simpler. The notification process could easily be made automated at a kiosk near baggage claim.

Quicker Processing. If the ASIR system is two-tiered in design, the passengers who volunteered to use the ASIR card should expect quicker processing through ticketing, security checkpoints, and boarding.

Airline Bonus Programs. Airline frequent flier or "VIP" cards could be combined into a special area for use by airlines. This will not be easy to implement as the airlines may not be overly willing to give up their existing cards due to their branding benefits.

Purchases/Rentals. One section of the ASIR card's memory could be allocated as an "electronic purse" and work as a debit card at airport vendors or for the in-flight purchase of liqueur or rental of headphones. This may be too ambitious a proposal, as it would further complicate efforts to get a program developed and implemented in a reasonable timeframe.

Special Service Advisory Codes. To alert aviation personnel of an individual's special needs. For example: Spanish speaking only, wheelchair required, blind, etc.