Full Testimony Transcript For Martin Huddart to Senate Subcommittee Report

HAND GEOMETRY BIOMETRIC SYSTEMS OFFER PROVEN RESULTS FOR AIRPORT SECURITY Written testimony submitted for the record by Martin Huddart, General Manager, Recognition Systems, Inc. before the Senate Aviation Subcommittee's Hearing on Airport Security Morgantown, West Virginia November 5, 2001

HAND GEOMETRY BIOMETRIC SYSTEMS OFFER PROVEN RESULTS FOR AIRPORT SECURITY

Written testimony submitted for the record by Martin Huddart, General Manager, Recognition Systems, Inc. before the Senate Aviation Subcommittee's Hearing on Airport Security Morgantown, West Virginia November 5, 2001

Good morning. My name is Martin Huddart and I am General Manager of Recognition Systems, Inc. I am pleased to be here today to discuss technology innovations and solutions that can enhance security at America's airports.

Recognition Systems, Inc. (RSI) is based in Campbell, California, the heart of the Silicon Valley, and was founded in 1986. It is a pioneer in the application of biometric systems. Our primary technology is Hand Geometry. The company's HandReaders have been installed in high security environments around the United States and worldwide for more than a decade.

Today, there are more than 60,000 RSI HandReaders around the world, reading millions of hands every day. RSI is a subsidiary of the Ingersoll-Rand Company, a diversified industrial manufacturer and a world leader in security and safety. Together, IR and RSI provide integrated security solutions – including hardware, biometrics and electronic technologies, software applications, maintenance and consulting services – to commercial and industrial markets and customers in the United States and around the world. Our products, technologies and security solutions can be found in over 90 percent of the nation's nuclear power facilities, at major airports and other high-security environments, including prisons, military bases, sports arenas, hospitals, government buildings, border crossings and universities.

In the wake of the terrorist attacks on September 11, one task is certain: we must significantly increase and improve the security of our air transportation infrastructure, and we must do so quickly. President Bush and Congress have proposed a number of solutions, and much of the subsequent debate has focused on issues of how we can better professionalize and supervise security personnel at airports. These are important initiatives. But we should also recognize there is a critical role for technology to play in providing enhanced security at U.S. and international airports. This was endorsed by the Secretary of Transportation's Rapid Response Task Force on Airport Security, established in the wake of the September 11 attacks. The Task Force recommended in its report of October 1 that airports take immediate action to better incorporate technologies into security procedures used to identify passengers, airport workers and crews, and for improved detection of arms, explosives and baggage screening. The Task Force also recommended that the Federal Aviation Administration (FAA) establish a public-private sector consortium to identify, sponsor and test new security-related technologies for our nation's airports.

The role of biometrics in airport security

Biometric systems lie at the core of technologies that can provide improved security at U.S. airports. Biometrics is the science of using physical characteristics to identify an individual. Modern biometrics systems were developed in the mid-1970s. Early commercial products were expensive and therefore limited to very high security applications, such as nuclear facilities and laboratories. In recent years, inexpensive microprocessors and advanced imaging electronics have greatly reduced the cost of biometric devices, while increasing their accuracy. These changes have made biometrics increasingly common in commercial applications. Today, thousands of businesses from day care centers to college dorms use biometrics for their access control needs, as well as for accurate personnel time and attendance monitoring.

Our hand geometry technology was specifically designed to be used in high-volume environments, where access must be tightly controlled and there is a need to provide forgery-proof identification procedures. Our technology has been engineered to work reliably in difficult security environments such as airports, which demand rock-solid performance even in outdoor applications. The accuracy, reliability, durability and successful track record of biometric hand reading technology is unparalleled in the industry.

Biometric hand readers simultaneously analyze over 31,000 points and instantaneously record over 90 separate

measurements of an individual's hand – including length, width, thickness and surface area – to verify that the person using the device is really who he or she claims to be. The hand reader compares this information with a "template" of the individual's hand that has been previously stored in the reader, on a server or on a card. Once the person has been identified as a valid user, a door can be opened, or access can be provided to an air operations area or to boarding a plane. The reading and verification process takes less than a second.

Proven vs. experimental technologies

Members of Congress and Federal and local aviation authorities are presently being inundated with proposals for new technologies that can be incorporated into the nation's air transportation system. This includes many different biometric systems, including hand, iris, fingerprint, facial and voice recognition.

While there is no disagreement that technology can enhance security at our nation's airports, we must also understand this is not the time to experiment with new and unproven systems. Only those technologies that have already been proven in the airport and travel environment, and which have an established reputation for reliability, should be in the forefront of our decision-making process as we consider how to proceed in the weeks and months ahead.

Decision-makers must understand that the different biometric technologies being discussed in today's new airport security environment are in various stages of development and not all have the same record of reliability and performance. Hearings like this are important for policy makers in Washington and airport officials around the country to better understand the scope of existing and new technologies, and to see and compare first-hand the relative advantages and disadvantages of different technology solutions.

We also feel it important to point out that we should not be looking for the one biometric technology that solves all the identification needs of our transportation system. This does not exist; there is no silver bullet. What should be done is to take the best of breed and apply them appropriately.

RSI participated in a demonstration of biometric security technologies sponsored on October 27 by Rep. Jim Matheson (D-UT) at Salt Lake City International Airport, which will serve as the gateway to tens of thousands of U.S. and foreign visitors attending the Winter Olympic Games in February. RSI demonstrated how our biometric HandReaders, when used with smart card technology, can be an integral part of an airport's integrated security system.

One fact is well established and should be clear: Of all the biometric systems currently in use, hand readers are the technology that today best meets the essential tests of performance and reliability in airport environments for employee access and high volume passenger verification .

It is important that the FAA, as the Federal agency with overall jurisdiction and responsibility for aviation security, take the lead in determining specific airport security technology standards to be adopted for individual airports. To facilitate this effort, Rep. Matheson and Rep. Mike Honda (D-CA) have introduced H.R. 3101, which would direct the National Institute of Standards and Technology (NIST) to develop standards and measures for aviation security technologies. The FAA would fund and carry out a pilot program in at least 20 U.S. airports to test and evaluate the effectiveness of various existing, new and emerging aviation security technologies, and then report on their findings and recommendations. These pilot projects will provide an opportunity to compare and evaluate different biometric systems.

We certainly support these pilot programs, but also know that they will take time. And time is our enemy. So we must have a short-term as well as a long-term strategy for the use of biometrics to enhance the security of America's transportation infrastructure. The short-term goal: Improved airport access control The Federal Aviation Administration (FAA) already directs U.S. airports to insure that only authorized individuals are allowed access to flight operations areas. Most airports implement this directive by using card-based access systems to control access to high-security areas. However, card-based systems are an inadequate technology to control access. These systems can only positively or negatively identify the card, not verify that it belongs to the individual using it. By contrast, a biometric system can truly verify the person.

For nine years, San Francisco International Airport (SFO) has been using RSI's HandReaders to meet the difficult challenge of securing access to sensitive areas of the facility. More than 30,000 airport employees are enrolled in the system which spans the entire airport and protects more than 180 doors. SFO has demonstrated the reliability of RSI's hand geometry technology in the airport environment over several years of use.

Using biometric hand readers to control airport-wide access not only enhances security, it provides confidence to airport employees by demonstrating that a major and obvious security need is being successfully addressed. It also increases confidence of the traveling public who can see this technology layer in place throughout the facility. This is not a pilot or demonstration project; it is a permanent, proven solution that lies at the core of SFO's security infrastructure. Therefore, with confidence, we can deploy our technology at every U.S. airport now and the enhanced security we provide at SFO can blanket the rest of our nation's airports.

To this end, current regulations governing access demand that only authorized people be allowed access. A clarification to this regulation (FAR 107.14a) is needed to ensure that it is being followed with the full and clear intent of the regulation, and calls

for the use of biometrics to achieve this goal.

A longer-term goal: Automated aircraft boarding systems

In the wake of September 11, Americans have experienced more complex and time-consuming security procedures at U.S. airports. Media reports have focused on passengers who have confronted long and slow-moving lines at airport security checkpoints. Most Americans recognize the need for new and improved security improvements and so far have been patient with the inconveniences they cause. But the reality is that the traveling public will soon demand ways to automate this new, higher level of security. This will be particularly the case with business travelers who need to fly frequently, and to whom long delays have an economic consequence.

One approach to this problem is for U.S. airports to segregate passengers into "high risk" and "low risk" categories. This allows airport security personnel to focus their time, attention and resources on a relatively small number of "high risk" passengers. By doing so, security processes can be eased for individuals who have been pre-determined to be at "low risk," and who make up the bulk of the traveling public.

This type of system has been in place for seven years as part of a pilot program of the Immigration and Naturalization System (INS). It is called INSPASS. Frequent travelers have a background check performed and upon passage of this they are entered into the program. A kiosk at U.S. immigration control is used to allow the INSPASS user to insert their identification card and enter appropriate flight information. Their identity is then confirmed by using an RSI HandReader. The live template of the user's hand is instantly compared with the template that has been previously stored in a secured government database. If the templates match, the individual can proceed. Over 23,000 transactions take place each month at nine separate North American airports.

A similar program is in use at Tel Aviv's Ben Gurion International Airport, one of the world's busiest air terminals and a facility recognized and respected around the world for its high level of security. RSI HandReaders are used in a system designed by Electronic Data Systems Corporation (EDS) that allows Israeli citizens and frequent international travelers to use an automated inspection and identification kiosk. Travelers use a credit card for initial identification; then the system instantly verifies their identity with a HandReader. The system prints a receipt that allow travelers to proceed.

Ben Gurion's biometric identification system has reduced long waiting times at security checkpoints. The automated inspection and identification process takes about 20 seconds to complete. By contrast, passport control lines at Ben Gurion can take up to an hour. The project was initially offered only to frequent travelers, but has recently been made available to all Israeli citizens. Nearly 80,000 Israeli citizens have enrolled in the program, and the system is now processing about 50,000 participants each month. In 2002, a similar biometric border crossing system will be installed at the Israeli/Palestinian border to verify the identity of 50,000 people who cross the Gaza Strip every day. Developing a similar system here in the United States was one of the core recommendations of the Secretary of Transportation's Rapid Response Team on Airport Security. The Rapid Response Team concluded "there is an urgent need to establish a nationwide program of voluntary, pre-screening of passengers, together with the issuance of 'smart' credentials, to facilitate expedited processing of the vast majority of air travelers and to enable security professionals to focus their resources more effectively."

(Recommendation #16)

We are confident that a similar system could be developed for U.S. airports and the Federal government and Congress should provide the leadership necessary to implement this concept. To this end, we recommend that the U.S. Department of Transportation conduct a study of options for improving positive identification of passengers at check-in counters and border crossings through the use of "smart cards" and biometrics, in an effort to determine the feasibility and cost of such a program and a schedule for requiring air carriers to put it in place. Using biometrics to verify immigration and visa status at U.S. airports

Biometrics can also play an important role in addressing short comings in the nation's immigration and visa systems. America's open borders have created ample opportunity for terrorists to enter the United States. Each year, more than 300 million individuals cross our borders. While for the most part these border crossings are legitimate citizens and visitors, the U.S. lacks the ability to track border crossings, or even to accurately confirm the identity of individuals entering or leaving the country. Legislation introduced in the U.S. Senate on October 25 by Senator Diane Feinstein (D-CA) and Senator Jon Kyl (R-AR) seeks to improve the ability of immigration officials to identify foreign visitors at U.S. airports and other border crossings by using biometric technologies. The legislation would develop a new biometric "SmartVisa" card that foreign nationals would swipe upon their entry and exit to the United States. To ensure that these cards correctly identify the individual who is authorized to use them, the bill would authorize funding for INS to deploy biometric card readers and scanners at all U.S. airports, seaports and land border crossings.

Here again, a similar system is already in operation in Israel. The Israeli Government is using RSI HandReaders in its BASEL border-crossing project. Paired with Visionic's facial scanning technology, this dual biometric system is designed to verify the identity of more than 50,000 individuals who daily cross the Israeli-Palestinian border. In an area of the world where citizens live with the fear of terrorism every day, and where there exists a need to manage border crossings with extraordinary reliability and accuracy, the fact that the Israeli Government has chosen RSI HandReaders for this task should serve as a positive endorsement that this system represents the best available technology for use in U.S. airports.

Conclusion

As our nation moves forward following the tragic events of September 11, the overriding security issue will be to better manage people and access within the complex environment of a commercial airport. Technology, even sophisticated biometrics, cannot replace improved training for security personnel and heightened human monitoring and vigilance. We know that even the most careful baggage screener can grow tired after hours on the job. And the most careful worker can mistakenly lose an ID card or a key. But a biometric hand readers will not fall asleep on the job; it will never take a day off; it won't allow airport employees to "piggy-back" behind authorized workers; and it won't "loan" its ID card or access code to cousins, friends or co-workers.

For these reasons, biometric hand readers offer a valuable solution to enhancing security for Americans who depend on our air transportation system and who today, and tomorrow, need to be reassured that those charged with the responsibility of providing for the public's safety have evaluated and utilized every available technology to do so.

Thank you.