



## **Complete Testimony Transcript For James J. Scott to Congressional Subcommittee**

### **Statement by James J. Scott President, Security and Safety Solutions, Ingersoll-Rand Company before the House Subcommittee on Aviation Thursday, October 11, 2001**

#### **Statement by James J. Scott President, Security and Safety Solutions, Ingersoll-Rand Company before the House Subcommittee on Aviation Thursday, October 11, 2001**

Good morning. My name is Jim Scott, and I am president of Ingersoll-Rand's Security and Safety Solutions business unit. I am pleased to be here today to discuss new innovations in technology that can enhance security at America's airports. In the wake of the attacks on the United States on September 11, we have a clearer understanding that improving security at airports means making changes in the way that airport personnel and airline passengers interact with each other. But we should also understand there is a critical role for technology to play in providing enhanced security at U.S. and international airports. President Bush and Congress have already proposed several important initiatives to improve security at airports around the United States. To enable security personnel to perform their jobs effectively, they must have the best and most state-of-the-art equipment and technologies to help them do their jobs. The deployment and use of available technological solutions in our airports is the focus of my remarks today.

Ingersoll-Rand is a world leader in four major industrial and manufacturing sectors. These are infrastructure development, industrial productivity, climate control and security and safety. We employ 50,000 workers around the world. We manufacture more than 30,000 different commercial and industrial products in 100 facilities in the United States and other countries. Our products are exported from the United States to 153 countries around the world. IR's annual sales in 2000 were \$8.3 billion.

Ingersoll-Rand's Security and Safety sector provides total solutions – including hardware, biometrics and electronic technologies, software applications, maintenance and consulting services. Our commercial markets include airports in both the United States and around the world, as well as other high-security environments, including power plants, universities, hospitals, sports arenas, prisons, government facilities, border stations and commercial buildings. Our product solutions include several leading and recognized brands, including Recognition Systems biometrics devices, LCN door closers, Steelcraft doors and frames, Von Duprin exit devices, Schlage locks, and Locknetics computer-managed, electronic locking systems.

IR security and safety products and solutions have an outstanding reputation in the industry for their reliability, durability and innovation. We are not just a manufacturer of hardware products. In fact, we work with architects and building contractors from the very beginning of construction planning to incorporate the right mix of security products and solutions, and customize security solutions for each customer.

I have not come today to promote IR products. Instead, I want to outline a vision for how technologies that are available today can be integrated and used to provide a higher level of security for managing all people at our airports.

Airports are among the most challenging environments to secure from terrorist activity. They comprise an expansive perimeter, with numerous points of access and numerous individual buildings and facilities, for which access must be provided for thousands, in some cases tens of thousands, of individuals every day. While much attention is currently being given to addressing security challenges relating to airline passengers, we must not overlook the need to improve and better integrate security efficiencies and monitoring of airport personnel – including flight crews, caterers, vendors, contractors, ground crews, maintenance workers, baggage handlers, and even parking attendants – in short, everyone going in or out of the secure perimeter that is the airport facility.

In addition, because commercial planes travel across an extensive global air transportation network, security standards that will be adopted and maintained by airports here in the United States must be replicated across the entire global air transportation system, including foreign airports, so as not to create weak points that can be exploited by terrorists. We have an enormous challenge ahead of us. Within an airport, there are areas that must be accessible to the public and areas that require different levels of secure access. Security must be provided not just for traditional access controlled points, but for cabinet and storage areas, vehicles, fuel supplies, control towers, parking facilities – any area where an explosive device or a weapon could be placed or hidden. Both airport facilities, as well as hundreds of individual aircraft, can be the target of terrorism. All must be protected.

A review of current airport security procedures and technologies across the United States today will reveal that there are numerous systems in place. Some are new and utilize state-of-the-art technologies, while others have been in place for ten or

twelve years and are outdated. Many airport security systems rely on identification cards, magnetic strip cards, PIN numbers, mechanical keys and mechanical push buttons. In most cases, these security devices work independently from each other. In almost all cases, they can be defeated. Identification cards can be forged. PIN numbers and codes can be borrowed or stolen. Keys can be duplicated.

The problem with these types of security products is that they are, in effect, "stand-alone" systems. Once defeated, there are usually no means of immediately determining that security has been breached, and no back-up system in place to prevent additional security violations.

Instead, what is needed is an integration of technologies and products throughout the airport environment that consolidates information, data and security devices into a common database. This enables airport security personnel to monitor every individual in an airport – from pilots and flight crews, to baggage handlers, to aircraft technicians, to vendors – and simultaneously provide customized access for each to only those areas where they are required to be, and only when they are required to be. The technology exists today to dynamically link individual work schedules to access authority – not just to physical areas of the airport, but to cabinets, storage areas, vehicles and equipment.

Biometric systems lie at the core of new technologies that can provide customized security, not just for access control, but for monitoring the movements and activities of people throughout the airport environment. Biometrics is the science of using unique physical characteristics to identify an individual.

The most reliable system currently in use is biometric hand readers that turn an individual's hand into a forgery-proof identification card. Other biometric systems that work by identifying fingerprints and facial features are in various stages of development. Biometrics hand readers simultaneously and instantly record 90 separate measurements of an individual's hand length, width, thickness and surface area. This technology uses microprocessors and advanced-image electronics to read the geography of an individual's hand and verify that the person using the device is really who he or she claims to be. The hand reader compares this data with the individual's hand "template" previously stored in a database. Once the person has been positively identified, a door can be opened. The process takes less than a second to complete.

In recent years, biometric systems have become more powerful and less expensive. They provide a very high level of confidence, as well as speed and convenience – far above other forms of identity checking. Biometric devices can also monitor personnel time and attendance, inventory and scheduling systems. This is a truly integrated system that not only provides a high level of security, but can enable organizational efficiencies and cost reductions.

Biometric systems are particularly effective in an airport environment. Take for example the problem of controlling access to a particular jetway. Several planes will use the jetway over the course of a day. Different flight crews, technicians and airport personnel will need access to the jetway, but only for a particular period during the day. By combining biometrics technology and personnel scheduling techniques, when an aircraft has left the jetway, the crew and personnel that serviced the departing plane can immediately be deleted from the system, and the next scheduled flight's credentials can be simultaneously activated. Access to that jetway can be restricted and controlled 24 hours a day.

Another example of how this technology can operate is to coordinate the movements of individual flight crews who must have access to more than one airport facility. A pilot who is on a short-hop schedule that will take him to as many as five or six different airports in a 24-hour period must now have an active identification card for each of these facilities. This requires them to carry multiple cards, each of which may use different technologies and processes. The technology exists to segment those on the ground from those who are in the air, and provide proper and secure access authority for each. For airline personnel who routinely move about our national air travel system, their credentials can be forwarded to where they are scheduled to fly, and activated for when they are scheduled to be in a particular facility.

Integrating this technology into a comprehensive security management system for airports is the vision that should be explored by Federal and local agencies, and this Congress.

In fact, some airport facilities in the United States and abroad are already using technologies. Biometric hand readers are in place in more than a dozen major U.S. airports, including New York's Kennedy International, and airports in San Francisco, Chicago, Miami, Newark, Los Angeles, Denver and Detroit. Similar systems are in place in Ben Gurion International Airport in Tel Aviv, Israel; Hamburg Airport in Germany, and the newly-constructed Incheon Airport outside Seoul, South Korea. Biometric hand readers are also used by the Israeli Defense Ministry, the Government of Lebanon and the Austrian Parliament in high-security facilities.

At Ben Gurion International Airport in Tel Aviv Recognition Systems' biometrics devices are a key element of a system similar to that being recommended by Secretary Mineta's Rapid Response Task Force on Airport Security (Recommendation #16). For that facility, we developed a national "smart card" program that allows Israeli travelers to be pre-screened and given credentials which, when presented at the airport, enable them to proceed with a less intense security process. This enables security officials at Ben Gurion to concentrate their resources on other passengers.

At the newly-expanded San Francisco International Airport, IR's Recognition Systems biometric hand readers have been installed at more than 180 separate locations. They comprise a critical component of the airport's overall security system. The

hand readers are tied to Locknetics' electromagnetic door locks. Security officials in San Francisco fully complied with FAA regulations that state that doors and access points should be released only to authorized individuals after they have identified themselves. They interpreted these FAA regulations to mean that simply presenting an ID card or a code is not adequate to determine that the individual requesting access is who he or she claims to be. A biometric device is the only proven safeguard to ensure that the person requesting access to a particular part of the terminal is indeed the person who has authority to go through that opening at that particular time.

In addition to securing airport facilities, we must also improve security in the airline cockpit. While a number of promising technologies are being discussed in this area, including the ability of control towers to take over flight operations of a hijacked airliner, the airline industry must now implement immediate solutions that focus on fortifying the aircraft door frame and cockpit door. Here again, technology offers solutions. In recent days, IR has contacted airline manufacturers and major U.S. air carriers to offer our technical expertise in the area of electronic locking systems that will secure access to the cockpit at all times.

Ingersoll-Rand can also provide technical assistance to the U.S. Department of Transportation and the Federal Aviation Administration. IR security professionals are available to provide technical and intellectual-property guidance to the task forces being established to evaluate existing airport security measures and propose new procedures and technologies. Specifically, we are prepared to participate in the Aviation Security Technology Consortium recommended by Secretary Mineta's Rapid Response Team on Airport Security (Recommendation #5). We agree that such a consortium of government and private companies can help identify, sponsor and test new technologies for airports. We would bring to this initiative our extensive experience, our position as an industry leader, and our commitment to helping the country in a time of need.

This is not the first time Ingersoll-Rand has responded in the wake of tragedy. Following the shootings and deaths at Columbine High School in Colorado, our company volunteered its security professionals to work with high school systems across the United States to evaluate their security procedures and recommend ways to enhance the safety of their classrooms and grounds.

As our nation moves forward from the tragic events of September 11, the overriding security issue will be to better manage people and access within the complex environment that is a commercial airport. Technology cannot replace improved training for personnel and heightened human monitoring and vigilance. We know that even the most careful luggage 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 reader will not fall asleep on the job, it will never take a day off, and it won't "loan" its access codes or ID cards to cousins or friends.

For these reasons, common database integration of systems linking people and their authority to access openings, and the inclusion of biometrics play a critical role enhancing security for Americans – for a nation who depends 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 in the air and on the ground have utilized every available technology to do so.

Thank you.