VOLUME 1, ISSUE 1, WINTER 2002 SPECIAL EDITION ON AVIATION SECURITY R&D

Federal Aviation Administration

R&D Review

Building a safe, secure, efficient, and environmentally compatible aviation system

Inside This Issue:

A MESSAGE FROM THE ADMINISTRATOR

The events of the past year have affected all of us in ways we never imagined, both personally and professionally. We are in the midst of profound change across a broad front.

We are laying the groundwork for the transportation legacy of the 21st century -- for an aviation system that safely, securely, and efficiently links the nation and the world. There is no more exciting, challenging, or difficult time for aviation.

In particular, we are entering a new era for aviation security. Aviation security, which had been the responsibility of the airlines, is now a federal responsibility, overseen by a new undersecretary of transportation for security. We at the FAA, however, are continuing to do our part, to support and ensure the success of the new organization.

The challenges we face in aviation security have never been greater. As you will see in this premier issue of FAA's *R&D Review*, we are working aggressively with the aviation community to exploit new technologies to further enhance our explosive detection capabilities. We are considering every available tool and every technology on the horizon to ensure that the tragic events of September 11, 2001, can never happen again.

Although I am confident that technology will play a stronger, more vital role in aviation security, we must keep in mind that technology alone cannot secure the aviation system. We must be ever mindful of the vigilance, competence and leadership of the human element.

To determine optimal security solutions (people and machines), we are working closely with industry and the academic community. Recently, at my request, the Security Subcommittee of the FAA's Research, Development, and Engineering Advisory Committee, reviewed more than 1,300 technology and other security suggestions that I had received from the public, industry, academia, and other government agencies. I cannot thank this group enough for their yeoman work. I am energized by the cooperation we are receiving. The work of this subcommittee is just one example of the ongoing commitment and dedication of our partners to ensure the national aviation system remains safe and secure.

With the new emphasis on advancing and improving security, R&D will occur at a faster pace than ever before. I am committed to keeping the aviation community apprised of agency R&D developments in security, as well as in safety, efficiency, environment and energy.

Jane Garvey

FAA
R&D REVIEW

R&D Review is published quarterly by FAA's Office of Aviation Research.

R&D Communications Manager
Theresa L. Kraus, Ph.D.

Editorial Staff
Louise Muniak
Cymando Henley
Karen Stewart

If you have a story or photograph you'd like to contribute to ***R&D Review***, or to be added to the mailing list, please contact:

Theresa L. Kraus
Federal Aviation Administration
Office of Aviation Research
800 Independence Ave., SW
Washington, DC 20951
(202) 267-3854
terry.kraus@faa.gov

A MESSAGE FROM THE DIRECTOR OF THE SECURITY R&D PROGRAM

In the aftermath of the tragic events of September 11, the FAA's aviation security research and development (R&D) program dramatically increased efforts to determine what security technologies were worthy of acceleration. We are working closely with our partners, in government, academia, and industry to determine which technologies have technical viability, offer a high payoff, and can be deployed quickly. Of particular interest are technologies that can work together to enhance the security of passengers, checked baggage, checkpoint baggage, cargo and mail in the entire airport and civil aviation environment.

When President George W. Bush signed the Aviation and Transportation Security Act (Public Law 107-71), into law last November, security, research, development and deployment changed forever. This law created the new Transportation Security Administration (TSA) that is required to strengthen the ability to deter, detect and defeat all threats to civil aviation. The Act has many important milestones, including achievement of 100% screening of checked baggage by the end of this year.

Introducing vital new security technologies into the National Airspace System and significantly enhancing the performance of current technology requires a well planned and coordinated effort. This important coordination and sharing of knowledge was one of the major benefits of the Third FAA International Aviation Security Technology Symposium held in Atlantic City, New Jersey, late in November 2001. When the 2001 conference was planned five years ago, it was primarily intended to be a technology discussion conference. After September 11, 2001, however, this valuable conference took on a radically increased urgency for new security R&D and airport deployment. Instead of basic technical networking, over 1,000 highly qualified world security attendees from government, industry, and academia conducted critically important national security R&D planning. This reflects the critical need to improve and advance vital transportation security technology. Also included is the need to reduce passenger delay and provide robust contributions to the nation's homeland defense.

This special security edition of FAA's Office of Aviation Research's *R&D Review* focuses on the important transportation security task ahead. It provides a quick look at emerging security technologies and a glimpse of some of the more important developments, deployments, and research inputs. Our Division's technology challenges are great, but we are dedicated to satisfy them in enhancing transportation security, the nation's economy, and our quality of life.

Paul Polski, Director
FAA Office of Aviation Security R&D

CHECKPOINT SECURITY

The First Line of Defense

One of the first lines of defense in aviation security is preventing passengers from carrying weapons, bombs, and other threats onto an aircraft. As Huban Gowadia, Ph.D., FAA's Office of Security Policy and Planning, pointed out at the security technology symposium, "screening at the checkpoint is made considerably more challenging because of its many parts. We must account for threats concealed upon people, in their carry-on items, as well as prevent breaches through the checkpoint and exit lane."

The challenge at the checkpoint is to detect weapons -- both metallic and non-metallic -- including explosives and possible chemical and biological agents. All these threats must be detected while maintaining an even passenger flow. This places a restriction on the screening duration and requires the minimization of false positives. It also means we will need intelligent architectures that will promote efficient throughput at the checkpoints. However, we will need to balance security with the passenger's right to privacy."

In a speech at the Summit on Homeland Security & Defense in late November, Secretary of Transportation Norman Y. Mineta emphasized these ideas, saying "our goal in passenger screening is no weapons, no waiting. We will strive to develop a screening process that prohibits weapons or other banned materials in airport sterile zones without requiring a wait of longer than ten minutes at any security checkpoint for passengers using U.S. airports."

Dr. Gowadia explained that the "only way we will be able to meet the challenge is if we incorporate an integrated focus. As always, threat analysis drives our work. But we cannot afford the luxury of our different resources working in isolated pockets."

Current checkpoint R&D focuses both on passenger and carry-on baggage screening. FAA researchers are working to enhance the detection capability of walk-through metal detectors. One way this is being accomplished is by instituting new self-qualification, verification, and calibration protocols for the machines.

No weapons, no waiting

Similarly, the FAA is also working to develop a new calibration aid for hand-held metal detectors.

Researchers are also developing new equipment for use at passenger checkpoint areas that will be able to: enhance the ability of metal-detection portals to operate effectively in an electrically noisy environment; provide better information to security screening personnel on the type and location of potential weapons on individuals who trigger metal-detection portal alarms; and increase the detection capabilities of existing systems by adding the ability to detect a broader spectrum of metals and alloys, plastic explosives, and other threat materials.

The FAA is deploying trace detection devices to airports across the nation. These units detect the presence of explosive materials by reacting to trace amounts of explosives and can detect a broad spectrum of plastic explosives and other threat materials.

Researchers are currently examining the efficacy of a similar technology in the form of document or token scanners to screen passengers. When a screener wipes such items with a swab and then places it into the scanner, trace amounts of explosives can be detected.

Nanotechnology and MEMS (microelectromechanical systems) are, however, the wave of the future. The FAA's R&D program already has several projects looking into the use of micro fluid sensors, microcantilevers, GC-based and IMS-based microsensors for the detection of explosives. Work in this area is promising.

For additional information, contact either Dr. Huban Gowadia, FAA Office of Aviation Security Policy and Planning, at huban.gowadia@faa.gov. or Mr. Lee Spanier, FAA Explosives & Weapons Detection R&D program at lee.spanier@tc.faa.gov.

BIOMETRIC TECHNOLOGIES

The Future of Aviation Security

Prior to September 11, you generally only saw biometric technologies in movies; now they might just be coming soon to an airport near you.

The FAA established a multi-agency working group to accelerate its study of the integration of biometrics into airport security systems, which is now one of the most commonly recommended technology areas for improving aviation security.

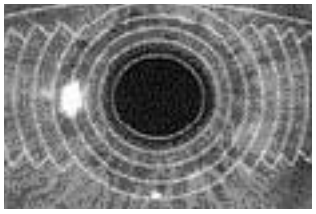
The working group identified four areas in which mature and proven biometrics can be used to improve aviation security: One, employee identity verification and access authorization to secured areas within an airport. Two, protection of airport public areas through surveillance. Three, passenger protection and identity verification. And, four, air crew identity verification.

The group, co-chaired by the Department of Defense Counterdrug Technology Development Program Office, has said that "the biometrics industry is on the threshold of providing a major infusion of new technology."

It is through this group that the FAA is working with the Department of Defense (DOD) and the National Institute of Standards (NIST) to begin a facial recognition evaluation program. The FAA Technical Center and the National Safe Skies Alliance have already begun working with the interagency Technical Security Working Group (TSWG) to evaluate biometric technologies.

According to Rick Lazarick (AAR-510), "biometrics are automated methods of recognizing a person based on physiological or behavioral characteristics. Examples include: fingerprint, hand geometry, iris recognition, facial recognition and speaker recognition."

Using biometrics devices, for example, to recognize employees provides a means to ensure access to secured areas within an airport is restricted to authorized personnel. Rick explains that, "This would greatly reduce the vulnerability to lost or stolen cards, and would be part of a system that could insure access to secured areas is limited to positively identified, authorized individuals."



Over 1.6 million passengers fly on commercial aviation every day in the United States. Any security system is built on trust. A Passenger Travel Identity card can guarantee identity using biometrics and facilitate the application of various databases to quantify the level of trust/risk for each passenger.

Such a decision will not be made in a discriminatory manner. This will allow us to spend the most time screening the passengers we trust the least. Aside from terrorists, this could also help prevent general identity theft, and better identify individuals classified as undesirable or prohibited passengers, such as air rage offenders. The technology could also possibly allow for travel histories of suspected individuals to be monitored and logged for interesting patterns or deviations.

Prior to September 11, the market for biometrics was relatively small compared to current sales anticipation to the aviation industry. Government organizations have only recently taken a close look at the efficacy of these technologies to address legitimate security concerns. Consequently, there 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.

There is a possibility that implementation of some of the applications would raise privacy concerns by the public. Airport and air carrier employees must have access to certain otherwise restricted areas 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. Since this is the case, enrollment into a biometric system could be a condition of

employment. Enrolling general passengers, however, would be a little more difficult. Because of all of the varying regulations between federal, state and local authorities, and possible religious conflicts for different groups, it would be all but impossible to make biometric security mandatory.

Two-tier security, where biometrics is an option, is an easy way to circumvent the regulatory challenge. Special incentives could be offered to those who participate in a voluntary biometric identity card program. Participating passengers would obtain or purchase an Aviation Security Identity Recognition (IR) card from an air carrier (similar to a Frequent Flyer card), or at a nearby airport (or U.S. Embassies for foreigners) to fly into/within the U.S.

Benefits other than increased safety could be added to a biometrics program. Passengers who volunteered to use the IR card should expect quicker processing through ticketing, security checkpoints, and boarding. Flight and baggage information could also be stored on the card, making airline notification or location of lost luggage much simpler.

Another problem with the use of some biometrics, at the present time, is their sensitivity to variations and interference. Speaker Recognition, an automated method of using vocal characteristics to identify an individual using a pass-phrase, is not widely deployed, partly because background noise affects its performance. Facial recognition can be foiled by something as simple as a head tilt or sun glasses, and system capabilities are significantly degraded under poor lighting conditions.

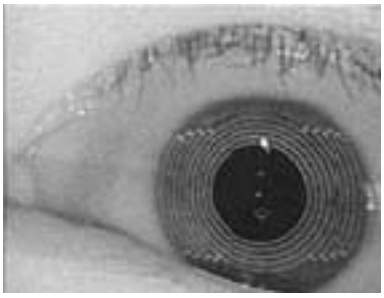
However, some forms are quickly gaining widespread support and approval. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users. During the 1996 Summer Olympic Games, hand geometry secured access to the athletes' dorms at Georgia Institute of Technology. During the 1998 Winter Olympics in Nagano, Japan, an iris recognition identification system controlled access to the rifles used in the biathlon.

In the airport environment, the National Safe Skies Alliance (a government-funded private research group in Knoxville) performed a study for the FAA evaluating the combination of card readers and fingerprint and hand geometry identification. San Francisco International Airport is currently using hand geometry for employee access control. And, the airport in Charlotte has evaluated iris recognition for use in both employee and passenger identity applications with high marks for acceptability.

Rick points out that "there are many unknowns concerning the content and distribution of biometric databases to support aviation security operations. There is no agreement on if there should be separate databases for each biometric application. Nor is there any agreement on where data will be stored, which agencies will have access to the information."

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. The FAA intends to coordinate a series of technology evaluations and operational demonstrations that will lead to standards for widespread implementation of these technologies.

For additional information, contact Mr. Rick Lazarick at rick.lazarick @tc.faa.gov.



CHECKED BAGGAGE SCREENING

FASTER, BETTER, CHEAPER

The agency's explosives and weapons detection research program is improving the systems used in airports for screening checked baggage. The FAA is currently working with industry to design next-generation systems that are fast and effective and provide a uniform, high performance level.

The challenge is greater than detecting an explosive -- the challenge is distinguishing an explosive from the things travelers pack in their luggage, to do so quickly and efficiently, and to do so with a manageable level of nuisance alarms.

To achieve this goal, the agency currently is pursuing development of viable explosives detection systems and other aviation security technologies that show promise of meeting or exceeding FAA certification performance standards, as well as creating advanced software, hardware modifications, and innovative techniques for existing systems.

Such research is on the cutting edge of technology, pushing the science to levels never before attained. For example, building on technology first used in the medical field, the agency has worked with manufacturers to adapt computed tomographic imaging, also known as CAT scan technology, to detect explosives in checked luggage.

These systems use transmission x-ray views obtained from a rotating gantry to map, segment, and characterize objects in luggage, identifying those objects that might be explosives.

Two vendors have met the FAA's certification criteria for explosive detection systems -- InVision Technologies and L-3 Communications.

InVision CTX-5500

L-3 eXaminer

CAT scan technology also is the basis for development activities focused on creating the next generation explosive detection systems (EDS) called ARGUS. ARGUS will be:

- Lower in cost
- Smaller in size
- Achieve Certified EDS detection performance
- Achieve Certified EDS false alarm performance
- Include threat image projection
- Accept all checked bags
- Simple to operate

The ARGUS program is designed to reduce significantly the acquisition cost of the certified EDS, which currently costs about $1 million per machine. ARGUS offers flexibility over the larger machines at a significant cost reduction.

The FAA funded three vendors to develop ARGUS in fiscal year 2000. This new technology will be capable of effective throughput of at least 50 checked bags per hour, and will cost approximately $300,000.

The systems will be deployed to small airports and smaller stations within large airports. The agency hopes to award a production contract for ARGUS in fiscal year 2001.

In addition to computed tomography, technologies currently employed in developmental efforts include x-ray diffraction, quadrupole resonance, multi-view x-ray, and advanced trace detection. Systems employing multiple technologies may surpass the performance of current generation CAT scan-based EDS.

The new security legislation will dramatically change the FAA's checked baggage R&D program.

The legislation requires that all checked bags be screened no later than 60 days after enactment of the law. Screening can be accomplished by:

- Certified EDS
- Bag match
- Manual search
- Canines plus other approved techniques
- Other approved means or technology

The legislation also requires that all checked bags be screened by EDS no later than December 31, 2002. According to Fred Roder, Ph.D., FAA's Office of Security Policy and Planning, this mandate necessitates that:

- Only existing EDS or EDS in the pipeline can be expected to be available in time;
- Few new starts for equipment or technology development will be considered;
- Any additional R&D funding will be designated for:
  --Argus
  --Raising the throughput and
  --Lowering the false alarm rate of existing EDS or systems and techniques in the pipeline.

For additional information, please contact Dr. Fred Roder, FAA Office of Security Policy and Planning at fred.roder@faa.gov.

Prototype May Enhance Air Cargo Security

Tests will soon begin on the prototype of a new automated prescreening system recently developed by the FAA Aviation Security Research and Development Division (AAR-530) to enhance cargo security on passenger flights. Similar to the computer system used to prescreen passengers, the cargo system will more accurately identify shipments that require enhanced security measures based on data provided by the shippers.

"Our objective is to provide security for cargo transported on passenger aircraft which is equal to that provided for checked and carry-on baggage and passengers," said Howard J. Fleisher, manager of the Aircraft Hardening Program and former program lead for air cargo security research and development (AAR-530), at the 3rd International Aviation Security Technology Symposium.

Continental Airlines integrated the prototype into its Cargo Reservation System upon its completion in September, but the FAA postponed tests because of the September 11 attacks. The FAA has revised its rules governing screening in cooperation with the Office of Civil Aviation Security Operations (ACO) and the system has been reconfigured.

There are more than 3,000 indirect air carriers whose business models vary significantly (small, single-location shops with a few steady customers; industry-specific and/or route-specific operations; large organizations with locations around the world and a wide clientele). Based on this variance, a "one-size-fits-all" approach to prescreening is not a practical solution.

Our objective is to provide security . . . which is equal to that provided for checked and carry-on baggage and passengers.

"The air cargo operational environment makes for a challenging screening regime," Mr. Fleisher said. "Computer-based prescreening systems may be appropriate for large indirect air carriers and air carriers."

About 80 percent of the cargo on passenger aircraft is handled by 20 percent of the companies, most of these are large companies.

"This system will not only guarantee security is done correctly, but will enhance [an individual company's] operation by receiving a decision much faster than, say, a manual analysis," Mr. Fleisher said.

By providing advanced warning of potential security delays and shorter "cut-off" for time-critical shipments, a computer-based solution like this one will:

- Provide process improvements (accuracy, speed, logistics management),
- Enhance security processing,
- Improve customer service.

The tests will last approximately six months and span Continental's global network. Both AAR-530 and ACO will participate in evaluating the new system.

For additional information, please contact Mr. Fleisher at howard.fleisher@tc.faa.gov.

SCENES FROM THE 3RD INTERNATIONAL

AVIATION SECURITY TECHNOLOGY SYMPOSIUM

HUMAN FACTORS R&D

ENHANCING HUMAN PERFORMANCE

The human operator is a critical component of current and advanced technologies to counter the threat of terrorism. It is clear that placing explosives detection equipment at airports is an important step in creating a secure aviation system, but it is equally necessary to ensure that the personnel who use the equipment are fully qualified and properly trained. To ensure a safe and efficient security system, the FAA's human factors research program is working to address operator capabilities, person-machine performance, and human-system (i.e., technology, people, procedures, and organizations) effectiveness for checkpoint, checked baggage, and cargo security.

The FAA's aviation security human factors research program is working to improve human performance in the aviation security system. Agency researchers are taking a three-pronged approach to increase human performance. First, because improvements in aviation security can be accomplished by adopting innovative, proactive methods of enhancing checkpoint screeners' contributions to overall security system effectiveness, researchers are developing innovative ways to improve screener selection and training. The goal is to ensure that security personnel (e.g., screeners, supervisors, law enforcement officers) have the necessary abilities, knowledge, and skills to detect and mitigate threats against civil aviation. The ability component focuses on identifying aptitudes, developing selection tests, and test validation. The knowledge component focuses on expanded and standardized training for checkpoint personnel. The skill component focuses on procedures development and validation, search strategies, alarm resolution, operational training and simulation, feedback, and performance monitoring.

X-ray Image Screener Selection Test (XISST).

Screener Readiness Test (SRT) Item.

A battery of screener selection tests, which includes visual-perceptual items and job sample items, has demonstrated validity in predicting screener detection performance. The job sample test, know as the X-ray Image Screener Selection Test (XISST), presents applicants with simplified X-ray images of bags which contain common target items (i.e., shoes, cell phones, keys). Applicants who are able to quickly and correctly identify these targets are demonstrating the abilities that are required to detect threats. This test will be an important tool in selecting applicants for federal screener positions.

A Screener Readiness Test (SRT) has been developed and validated to ensure that screeners master the knowledge and skills imparted during initial training. A comparable achievement test has been developed to assess learning during the period of On-the-Job (OJT) training required of each screener. Procedures and metrics for measuring and improving screener performance are also being expanded. These procedures and metrics have been the basis for detailed Efficiency and Effectiveness (E&E) evaluations of screeners to ensure conformance to procedures and to assess the types of errors that are made. This effort is consistent with the development of an error management system and improved quality assurance.

For example, to improve screener vigilance, provide embedded training or real-world threats, and assess

Fictional gun projected into a passenger bag. Note: feedback to the screener is provided in the top box and white highlights.

screener performance, agency researchers have developed Threat Image Projection (TIP) software for X-ray machines. The TIP system superimposes different types of threats into the stream of passenger baggage at a checkpoint. The system overlays a threat image (i.e., a knife) from an extensive library of images onto the X-ray image of actual passenger baggage being screened. The image appears on the monitor as if a threat object actually exists within the passenger's bag. TIP is an integral part of developing performance measurements and standards for screeners. It exposes screeners to threats on a regular basis to train them to become more adept at detecting threats and to enhance their vigilance.

The second human factors approach is to improve performance of the operator by designing equipment and machine interfaces that maximize perceptual, cognitive, and physical abilities of users while minimizing errors. The goal is to ensure that security equipment is designed and used consistently with human physical and cognitive capabilities. The design, development, evaluation, and use of security equipment must be based upon the role, capabilities, and limitations of human operators. Some specific issues include: interface design, usability, controls, displays, safety, fatigue, allocation of functions between the person and the machine, supervisory control and awareness of equipment status, operability, and maintenance. Security equipment must consider how, when, and what the human operator's role is to ensure the highest performance of the person-machine system. To address usability requirements, researchers are becoming involved in the system definition or conceptual design phase of new equipment. By being involved early in the design phase, significant improvements can be made to equipment without a major impact on schedule or budget. Furthermore, early human factors involvement increases the likelihood that the system will be easier for the user to operate.

Human factors evaluation of a prototype 3-D X-ray machine.

Laboratory acceptance testing of TIP-ready X-ray machines in support of Security Equipment Integrated Product Team procurement.

This program also conducts usability assessments of all new aviation security equipment and training systems to ensure that they are free of deficiencies and capable of effective and efficient operation by the end user. During these assessments, emphasis is placed on the capabilities and constraints of the operators and how they influence system operation. A laboratory assessment of multiple security imaging systems is currently being conducted. These systems use microdose X-ray to penetrate clothing to determine if a person is concealing a threat. The human factors assessment is focusing on threat detection, interface, resolution procedures, and passenger acceptance.

In addition, the final phase of assessment of the new ARGUS (low cost Explosive Detection Systems for smaller airports) is a System Qualification Test (SQT). The SQT will assess the training, usability, operability, and overall person-machine performance of each vendor's ARGUS prototype. This structured testing will ensure that new security technologies are usable by the screener population prior to deployment.

The third approach is improving the performance of the overall security system which is highly dependent upon human operators. The goal of enhancing the human system is to address the macro-level issues that have an effect on the performance of individuals, teams, and organizations to successfully identify and mitigate threats to civil aviation. These efforts ensure that security system designs and operations consider human factors issues of: fatigue, deterrence, information management, integration, organizational issues, management, compensation, architecture, error management, performance assessment and feedback, throughput, workload, stress, supervision, turnover, conflict resolution, oversight, coordination, and situation awareness.

For additional information on the agency's security human factors research program, contact Dr. Eric Neiderman, program manager for aviation security human factors R&D at eric.neiderman@tc.faa.gov.

A HISTORY OF THE SECURITY R&D PROGRAM

TERRORISM HAS CREATED ONGOING CHALLENGES

For more than 30 years, the FAA has worked to ensure the security of the Nation's civil aviation system. In its early years, those efforts focused on countering the hijacking threat, and included research and development of weapon detection technologies and equipment. Following a series of hijacking incidents in the 1960s and early 1970s, public and congressional interest in aviation security increased.

In 1974, Congress passed laws strengthening the FAA's mandate to ensure civil aviation security. Among other things, the legislation empowered the Secretary of Transportation, with the approval of the Secretary of State, to impose sanctions against the air carriers of nations that failed to maintain minimum security standards in the transportation of persons, property, and mail, as required by the Convention on International Civil Aviation. It also directed the FAA to require passenger and baggage screening procedures and law enforcement support.

In the 1980s, civil aviation faced the challenge of increased lethality in global terrorism, and the FAA responded by focusing on improving baseline security for international threats and taking action to protect U.S. carrier operations at foreign stations. The 1985 hijacking of TWA Flight 847 and a series of aircraft bombings showed that Americans faced a significant and lethal terrorist threat while flying abroad.

Hijacking of TWA Flight 847.

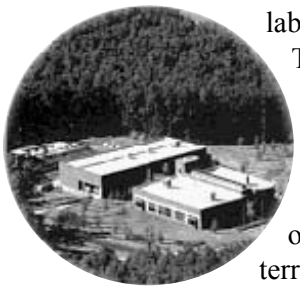
Pan Am 103 wreckage.

Unlike previous attacks, where terrorists destroyed aircraft but minimized casualties, the intent to cause mass casualties now became evident and helped to solidify public and congressional support for a strong FAA civil aviation security program.

The International Security and Development Cooperation Act of 1985 authorized the use of five million dollars from the Airport and Airways Trust Fund for research and development of airport security devices and explosives detection techniques. It also mandated a system for conducting security assessments at foreign airports, and authorized Federal Air Marshals as a permanent FAA workforce. The FAA also reorganized its civil aviation security organization to reflect its expanded responsibilities, creating international Civil Aviation Security Field Offices and the Office of Intelligence.

As the FAA worked to enhance security, tensions continued to mount abroad. In June 1985, a bomb exploded on an Air India flight, killing all 329 persons aboard. Six months later, two near-simultaneous terrorist attacks on airports in Rome and Vienna added urgency to the FAA's work to protect U.S. citizens abroad. Those attacks caused the deaths of 20 people and injured approximately 120. Five of the victims killed were U.S. citizens. As a result of this type of ongoing terrorism and the bombing of Pan Am Flight 103 over Lockerbie, Scotland, on December 21, 1988, the President's Commission on Aviation Security and Terrorism recommended that the FAA pursue a more rigorous program in aviation security research and development, and take other steps to counter the terrorist threat to the civil aviation system.

The Aviation Security Improvement Act of 1990 provided new authority for the FAA to strengthen aviation security through accelerated research and development. As a result, the agency intensified its research and development efforts to enhance aviation security and in 1992 opened an expanded security research



laboratory at its Technical Center in New Jersey.

In the 1990s, various plots by terrorist organizations revealed that U.S. air carriers remained prevalent targets of international terrorism. In addition, the nature of terrorism itself began to change. Previously, terrorist organizations had been primarily state-sponsored and, therefore, had operated in a highly structured fashion, with strict command and control.

As such, intelligence agencies -- whose work is critical to the success of the aviation security program -- could reasonably monitor the activity of those groups once they were identified. This enabled the intelligence community to detect indications of plans to attack, and provided the Federal government an opportunity to institute specific countermeasures commensurate with the likely plot.

In the 1990s, however, more loosely organized terrorist cells began to emerge and became more prevalent in the United States, as evidenced by the bombing of the World Trade Center in New York City. Additionally, terrorists with more individual goals and charismatic leadership styles, such as Usama Bin Laden, came to the forefront. Not constrained by the historical structure of state-sponsorship, these cells present new challenges to the intelligence community and present a new variable in the FAA's plan for protecting passengers and aircraft in air transportation.

In an attempt to understand better the changing threat, the Baseline Working Group, created by the FAA's Aviation Security Advisory Committee and composed of representatives from Federal agencies, industry, and public interest groups met on July 17, 1996. They began reviewing the threat assessment of foreign terrorism within the United States, considering the warning and interdiction capabilities of intelligence and law enforcement, examining the vulnerabilities of the domestic civil aviation system, and considering the potential consequences of a successful attack. That same evening, TWA Flight 800 crashed shortly after takeoff from New York's John F. Kennedy International Airport. Although the TWA Flight 800 tragedy was not the result of a terrorist act, it nonetheless caused both the White House and the FAA to reflect on the current threat and the best ways to deter future terrorism.

Shortly after the TWA tragedy, President Clinton created a White House Commission on Aviation Safety and Security chaired by Vice President Gore. The President tasked

the group to develop a strategy to improve aviation safety and security, both within the United States and abroad. In its final report, the Commission made it clear that criminal acts against civil aviation over the past few years have demonstrated that terrorists have an increasing level of knowledge in the design and deployment of explosive devices. The U.S. aviation security system must be capable of adapting to meet any and all new challenges. Congress responded by passing several pieces of significant legislation, which required certain actions be taken to improve aviation security.

Much of the FAA's pre-September 11 civil aviation security policies and regulations are the result of this history. It is clear, however, in the wake of the terrorist attacks, civil aviation security initiatives will change dramatically as the nation works to address a multitude of threats. This tragic event and the vulnerabilities it exposed are already watershed events that will drive the development of the aviation security system in the next decades.

THE REDAC AT WORK

PROVIDING CRITICAL INPUT

REDAC Security Subcommittee Chairman, John Klinkenberg, briefs the committee.

In October, FAA Administrator Garvey requested the Aviation Security Subcommittee of the agency's Research, Engineering, and Development Advisory Committee to form a Technology Assessment (TA) Team. The Administrator tasked the team to review the approximately 1,300 technology suggestions submitted by the American public and industry after September 11 and to review, in light of those suggestions, the ongoing FAA and relevant Federal Government research.

Because of the sheer volume of ideas and suggestions to improve security, the TA did not review each individual proposal, but rather looked at broad concepts and categories of ideas. To facilitate that review, the TA, lead by subcommittee chairman, John Klinkenberg, Vice President of Audit and Security for Northwest Airlines, divided into six groups:

- Airport Screening Checkpoints -- lead by Nick Cartwright and Colin Drury.
- Aircraft Hold Areas and Cabin Supplies -- lead by John Pennella.
- Aircraft Security/Hardening and ATC -- lead by Steve Luckey.
- Data and Identification Systems -- lead by John Klinkenberg.
- Airport Security -- lead by Hans Webber, President and CEO, TECOP International, Inc.
- Forward Looking Issues -- lead by Len Wolfson.

While proceeding with their reviews, John Klinkenberg advised the subteams "to think out of the box." He cautioned team members to keep in mind that "there is no silver bullet," no one remedy that will resolve all aviation security concerns.

The TA gave its initial briefing to the Administrator on November 20. In that briefing, the TA members pointed out that aviation is an attractive target for terrorists because of its high visibility. Attacking the U.S. national airspace system allows terrorists to increase the world's exposure to their various agendas. Because attacks on the airspace system can take many different forms, the TA team advised that the FAA needs to approach aviation security as an integrated system, with the recognition that in the short term less than perfect approaches will need to be adopted.

The team came up with a list of possible threats that could be addressed by new and improved technologies:

- Threat of putting explosives on board aircraft in checked or carry-on luggage - or by airport personnel - to be detonated during flight.
- Threat of sabotage to aircraft.
- Threat of explosives from truck bombs placed outside terminals and luggage/suicide bombs inside.
- Threat of attack on airport facilities and aircraft from within and outside the airport perimeter.
- Threat of putting on board aircraft biological/chemical agents for release during flight.
- Threat of release of biological/chemical agents in airport terminals.
- Threat of cyber attack on airport and air traffic computer systems.

Among its list of suggestion on how to improve security, the TA team recommended a series of actions, including:

- Enhancing the tools/equipment available to and screeners' performance at screening check point.
- Developing new, more effective screening technologies and procedures that will not inconvenience passengers.
- Introducing a frequent traveler positive identification process and establishing procedures and access controls to more effectively manage the risk associated with the relatively small percent age of travelers that do a large percentage of the actual travel.
- Establishing procedures, access controls, and inspections to prevent unauthorized materials/items from getting into the secure area via the screening

checkpoint or any other secure area controlled access points.

- Developing technologies, procedures and access controls to identify positively individuals before granting access and to deny unauthorized personnel access to the secure area.
- Establishing procedures and access control barriers to prevent and contain any overt attempt by armed individuals to force a penetration of the secure area.
- Introducing new inspection equipment to check all carry-on bag gage, and any other items being brought into the secure area for explosives, weapons, chemical/ toxic, and biologic contamination.
- Placing surveillance cameras to monitor areas near and around the screening checkpoint for suspicious activity.

From left to right: Dr. Herman Rediess, FAA Director of Aviation Research; Dr. Deborah Boehm-Davis, Professor of Psychology, George Mason University and REDAC Chair; and Mr. Steve Zaidman, FAA Associate Administrator for Research and Acquisitions.

Parked aircraft, especially ones that are unattended, are also at risk of being tampered with. Sealing these aircraft can help keep unwanted people and materials out. Options range from tamper-proof tape to mechanical locking devices. A monitored alarm system could also be used.

The team pointed out that people are one of the best resources when it comes to protection. A properly trained crew is the best option for performing pre-flight search of aircraft, because they spend so much time on them, according to the TA team. Additionally, since their job and, more importantly, life depends on a safe environment, they have a more vested interest.

As with all recommendations, the team acknowledged that it will not be easy to implement the gamut of suggestions. For example, there are issues, such as:

- Availability/timing to assure biometrics resources are accessible and usable on demand for positive identification.
- Privacy -- Will some of the new security concepts be acceptable?
- Logistic Realities - Can the technology handle the number of travelers?
- Timing -- Performance/processing time needs to be demonstrated to ensure operational satisfaction.
- Costs - What equipment, software and personnel are needed for implementation?

Despite such issues, the TA members urged the FAA to work with the new Transportation Security Administration to implement immediately two test beds, one at a large airport and one at a small airport, to integrate new and improved security technologies and procedures. At these testbeds, for example, technologies could be combined to reach the explosives detection goal, advanced personnel screening technologies could be tested, and checkpoints could be reconfigured to integrate all security systems and procedures to minimize disruptions to the air carriers, airports, and passengers.

FAA's Research, Engineering and Development Advisory Committee, established in 1989, advises the Administrator on research and development issues and coordinates the FAA's research, engineering and development activities with industry and other government agencies. The committee considers aviation research needs in air traffic services, airport technology, aircraft safety, aviation security, human factors, and environment and energy.

A maximum of 30 members may serve on the Committee, representing corporations, universities, associations, consumers and government agencies. Members serve two year terms. Dr. Herman Rediess, FAA's Director of Aviation Research, serves as the executive director of the committee.

For additional information on the committee, please contact Ms. Genia Embrey-Brock at genia.embrey-brock@faa.gov or Ms. Gloria Dunderman at gloria.ctr.dunderman@faa.gov.

A NEW WAY OF DOING BUSINESS

PARTNERING FOR SUCCESS

It is no secret that a team can accomplish more than a single individual or agency. With this in mind, FAA's security R&D program is working cooperatively with a number of domestic and international industry partners, academia, other government agencies, private industry, and even other governments. In fact, the FAA's security R&D program currently has a total of 48 active grants, 8 cooperative research and development agreements (CRDA), 5 Memoranda of Understanding (MOU), 1 Memorandum of Agreement (MOA), 2 Memoranda of Cooperation (MOC), and 5 reimbursable agreements.

At the Third International Security Symposium, held in New Jersey in November, these numerous partnerships were quite evident. A key partner, the National Safe Skies Alliance (NSSA), co-sponsored the symposium. NSSA, established in 1997 to assist the FAA and other agencies in meeting evolving needs in aviation safety and security, provides affordable, verified solutions to problems identified by the aviation community. Safe Skies receives a portion of its funding from the FAA, and is currently integrating and testing new security equipment at McGee-Tyson Airport in Tennessee.

In addition to its work with NSSA, the Aviation Security R&D division (AAR-500) is doing its part to reach out to academia and industry through a variety of innovative cooperative partnerships. FAA researchers, for example, are working with the Israeli Security Agency to determine the best means to strengthen the flight deck bulkhead and doors.

The FAA and the National Institute of Justice have recently signed a MOU to facilitate joint development of a concealed weapon detection technology.

Ancore cargo inspector.

Ancore Corporation is helping to develop a new air cargo inspection system under a recently signed (January 12) cooperative agreement. Ancore says their cargo inspector can detect explosives, narcotics, alcoholic beverages, and and other hazardous and environmentally sensitive materials. It can also be effectively used to inspect air cargo and passenger luggage, full-size marine cargo containers, loaded freight trucks, freight trains, and passenger cars.

Raspiscan manufactures metal detection systems like the AMD750.

Rapiscan Security Products Inc., is currently working with the FAA under a cooperative agreement to improve x-ray inspection of both checked and carry-on bags; the work is scheduled to be completed in September 2002. Rapiscan is a supplier of x-ray screening and explosive detection systems.

The FAA also has a dual partnership with Sandia National Laboratory and Syagen Technology. Researchers from all three organizations are working together on a new portal to screen passengers and personnel for explosives and chemical weapons.