Chapter 5

Human Factors in Aviation Security

Contents

Box

Chapter 5
Human Factors in Aviation Security

INTRODUCTION

Human resources are critical to aviation security. Security personnel—passenger and baggage screeners, guards and law enforcement officers, and airport and airline employees in general-are important elements of a system that prevents and deters hostile acts against air carriers. Technology can enhance, but cannot replace, the capabilities of these people and the many services they provide. Moreover, management practices based on behavioral research findings can further improve human performance.

This chapter considers the function of screeners in weapons and explosives detection, and the role of guards, officers, and other aviation employees in discovering (and deterring) suspicious individuals or situations. Within the past 20 years, technology has greatly increased the capability and productivity of these security people. Metal detectors and x-ray devices are faster, more accurate, and more socially acceptable tools for screening passengers and baggage than manual searches. Remote television and other monitoring devices, computer-controlled access to restricted areas, and communication and data systems allow comprehensive surveillance and threat assessment. While these technologies raise the capabilities of a security system to new levels, their ultimate success and actual performance depend on the people who design, operate, and maintain them.

Many security assignments require repetitive tasks and close monitoring for rare events—functions that humans perform poorly. Selecting well-suited individuals, training them properly, designing their work environment and rotation schedule to elicit the best possible performance, and providing motivating incentives are fundamental requirements for successful operations, regardless of the type of technology in place. These functions involve human performance; application of human factors in these cases can greatly improve the utilization of technology for airline security.

Dramatic accidents caused by human errors in the nuclear power, chemical, and transportation industries have increased public attention to human performance issues during the past decade. Additional training requirements, revised operating procedures, warning devices, and expanded government oversight are typical recommendations following accident investigations. However, these stopgap measures address only the surface of problems that are rooted in the complex interactions of people and equipment within the larger system and the institutional and organizational structures and procedures that drive the planning, design, and management of these systems. Following the ground collision of two jetliners in Detroit in December 1990, Dr. John Lauber, a member of the National Transportation Board, said that "basically the [aviation] system, the way we're operating it, almost demands nearly error-free [human] performance. ' Similar concerns can be echoed for the aviation security system—a number of successful airline terrorist events have been traced to a human failure.[2] "The challenge is to design a system. . which is tolerant of those errors when they do occur and which detects and traps them before we have [a catastrophe]. "[3] Multilayered defenses are employed at many commercial airports and airline terminals, and security managers and government authorities are turning to new technologies to buttress these systems. Heretofore, Federal requirements and industry use of security technologies have usually been with specific functions in mind. As long as the technical goals could be met effectively, the equipment was considered satisfactory and human performance problems related to the technology were resolved through revised training and procedures. Technology use in counterterrorism will likely increase dramatically over the next decade, but if early and

[1]John Lauber quoted by John H. Cushman, Jr., "Test for Aviation: Coping with Human Shortcomings," *The New York Times,* Dec. 10, 1990, p. A17.

[2]One example was the destruction of a Korean Air Lines flight over the Andaman Sea by a bomb planted by North Korean agents. The device, in a carry-on bag, was ahnost detected at a security checkpoint in Baghdad at an earlier stop. When a security guard wished to remove the batteries from a radio, one terrorist turned the radio on, proving it operated, and then raised a hue and cry, yelling and complaining. Instead of using this as a reason to stop the two suspect individuals and to examine their belongings minutely, the security forces decided to avoid trouble by allowing them to proceed.

[3]Lauber, op. cit., footnote 1.

methodic attention is not given to human performance issues, we may expect that system efficiency and effectiveness will be substantially impaired.

Background on Human Error

The human role in a security system is complex; thus the nature of human errors, from mental to physical, varies widely. Mental or cognitive errors can include improper judgment or decisionmaking, while physical errors may stem from motor skill deficiencies or faulty equipment design. A combination of physical and mental processes may influence other kinds of errors, such as those involving communication, perception, or alertness.

Human factors, a discipline combining behavioral sciences and engineering, focuses on improving the performance of complex systems of people and machines. Designing and operating a system so that it does not induce human error (in fact, designing it so that human error may be minimized) is one critical component of human factors and limiting the impact of a human error once it occurs is another aspect.

Many types of human error are systematic, following certain predictable patterns; once these patterns are identified, countermeasures can be developed. For example, poor location of switches or dials can induce manual or perceptual errors. For those types of human error that do not follow predictable patterns, mitigation techniques are difficult to develop. Some examples of mitigation techniques include automatic monitoring and warning devices. These subsystems, when properly designed and implemented, can be invaluable tools for negating human error.

Employee selection—allowing into the system only those people least likely to make mistakes—and continued quality control maintained through training and monitoring are basic steps for minimizing human errors. Potential errors can be forestalled by the use of standard procedures and checklists for routine and emergency tasks, planning work shifts and assignments so as not to induce inattention and fatigue, and properly designing the work environment. "If human factors engineering is done properly at the conceptual and design stage, the cost is high, but paid only once. If traning must compensate for poor design, the price is paid every day. "[4]

According to one expert, there does not appear to be a strong need for new basic research in human factors related spectifically to security-behavioral science findings in general and experience with human performance problems in other industries are probably sufficient to enhance current security operations.[5] For example, such knowledge is being used to upgrade security screener selection by airlines, and to improve training standards. However, the mechanisms to identify early on and to address effectively the human performance issues stemming from new security technologies, such as explosives detection systems, are not yet in place in industry or the Federal Government.

Shifting boring and repetitive tasks that people perform poorly to machines is an approach that can reduce errors. However, automated devices (or any new technology) may create new sources of human error.[6] Excessive false alarms unnecessarily distract operators and may lead to the device being ignored or disabled. During unusual or emergency circumstances, the lack of flexibility in many automated systems can be a serious limitation and the human backup may not be mentally or physically prepared (or possibly even capable) to take over. Consequently, a full system approach is required for reducing total human errors.

FAA AND HUMAN FACTORS

FAA Policy and Plans for Human Factors and Aviation Security

In a report released in July 1988, OTA concluded that FAA attention to the spectrum of human performance problems in commercial aviation fell far short of the level warranted, since human error is the leading cause of aviation accidents.[7] Later that same year, Congress passed the Aviation Safety

[4]Earl L. Wiener, "Cockpit Automation' *Human Factors in Aviation*, Earl L. Wiener and David C. Nagel (eds.) (San Diego, CA: Academic Press, Inc., 1988) p. 454.

[5]H. Clayton Foushee, Chief Scientific and Technical Advisor for Human Factors, FAA personal communication, 1991.

[6]See Wiener, op. cit., footnote 4, ch. 13 for a discussion of new and subtle types of human error that have resulted from the introduction of automation into aircraft cockpits.

[7]U.S. Congress, Office of Technology Assessment, *Safe Skies for Tomorrow: Aviation Safety in a Competitive Environment*, OTA-SET-381 (Washington, DC: U.S. Government Printing Office, July 1988).

Research Act, which directed the FAA to expand its research efforts on human performance in aviation and authorized funds specifically for that purpose.[8] The FAA responded by creating the position of Chief Scientific and Technical Advisor for Human Factors, responsible for coordinating for the FAA various human-factors research efforts within the FAA NASA, and the DOD and for opening lines of communication within the FAA and industry. Communication among Federal agencies is critical, since decisions made by the aviation industry and the operational and regulatory sections of the FAA often drive the need for new human-factors research and could benefit from an understanding of human-factors research findings and products.

The FAA has made progress in addressing the earlier criticism of its human-factors programs and understanding in aircraft and air traffic control (ATC) equipment and operations. However, the key shortcomings in FAA human-factors efforts that OTA cited in its 1988 study-insufficient agency expertise, uncoordinated research efforts, and regulations and certification standards that do not reflect human-factors principles-still exist within FAA civil aviation security programs. During the course of its study, OTA examined closely many of the technology development programs and regulatory efforts underway in the security sections of FAA and found a general lack of awareness and understanding of the human-factors issues involved with possible new security technologies. An exception to this situation, however, and a hopeful indicator of a new trend, has been the hiring of a human-factors expert at the FAA Technical Center to oversee human-factors research as it relates to airline security.

However, at present, it appears that the FAA is ill-prepared to identify and address possible human-factors concerns with the increasingly complex and diverse security technologies now under development. The dearth of trained human-factors specialists in areas of the FAA responsible for civil aviation security is a serious deficiency. Until recently, the Aviation Security R&D Service of the Technical Center would have merited similar concerns, but this shortcoming is being redressed, at least in part. Some of the expertise that the FAA is developing on human factors for other uses could also be applied to security issues.

One potential vehicle for bringing human-factors knowledge into aviation security efforts is the National Plan for Aviation Human Factors (HF Plan), the first major product of the heightened FAA attention to human performance issues following the enactment of the Aviation Safety Research Act. The HF Plan identifies significant human performance issues and lays out a 10-year blueprint for establishing and coordinating research programs and conveying the results across Federal agencies and industry. The HF Plan's development depended strongly on advisory committees composed of a cross-section of research, operational, and regulatory representatives from government and industry and approximately 50 of the nation's leading human-factors researchers.[9]

The good news for aviation security is that the Plan appears to provide a strong foundation for multi- and cross-disciplinary efforts and understanding in human factors and has begun to institutionalize and focus consideration of human-factors issues in FAA decisionmaking. The bad news is that nowhere in the Plan is security mentioned—the Plan addresses the following five aviation environments only: aircraft flight deck, air traffic control, aircraft maintenance, airway facilities maintenance, and flight deck/ATC integration. This should not be construed as criticism of the general thrust of the HF Plan—the human-factors categories considered have historically been more critical to aviation safety and are considerably more complex than human performance issues in security-and it is beyond the scope of this study to analyze in detail the specifics of the HF Plan. **However, some objectives and products of the HF Plan maybe directly transferable to aviation security, provided that lines of communication are established and security experts are included in committee structures.**

The Plan has eight objectives, all of which can apply to aviation security, but the following two are especially pertinent, given the present attention to technologies for countering terrorism:

. to encourage the development of principles of 'human-centered' automation and the design of

[8]Aviation Safety Research Act, Public Law 100-591.

[9]U.S. Department of Transportation Federal Aviation Administration, "The National Plan For Aviation Human Factors," vol. I, draft, November 1990.

advanced technology that will capitalize on the relative strengths of humans and machines;
. to develop human factors-oriented validation and certification standards for aviation system hardware and personnel that will enhance both safety and efficiency .10

The HF Plan is designed to be reexamined and revised periodically and aviation security could be added explicitly as a focus area if need and resources warrant.

Crucial to the development and future success of the HF pian is the Human Factors Coordinating Committee (HFCC), formed by the FAA administrator in September 1989.[11] HFCC has representatives from each major division of FAA and serves as "an advisory body for senior management of FAA in all matters involving human performance and [is] intended to assure that human factors issues are represented in all FAA activities. ' '[12] Until very recently, the Assistant Administrator for Civil Aviation Security was not represented on this committee.[13] However, this omission has since been rectified.

FAA Requirements for Aviation Security: Human-Factors Implications

Aviation security personnel and equipment have not received (and have not needed) the same level of regulatory and certification attention that the FAA places on flightcrew, air-traffic controllers, and ground support personnel and their respective aviation equipment. The FAA has focused its regulatory efforts on elements of the aviation system essential to flight safety. For example, the performance of pilots and aircraft systems are continuously critical for maintaining safety-a failure could cause an accident. On the other hand, the performance of the security system (other than as a deterrent) is rarely critical-flight safety is at risk only when security performance fails at the same time that a threat occurs. Moreover, FAA staff and the agency "culture" are predominantly interested in aviation technology and operations and protecting facilities and countering terrorism are not an inherent part of aviation.[14] However, the increasing Complexity of screening technologies and the continuing (possibly increasing) terrorist threat make the performance of aviation security systems more critical to flight safety.

Aviation terrorist events in the 1980s made apparent the shortcomings of the minimum Federal security requirements. The FAA and the airlines both focused attention on screener selection and training, detection and screening technologies, and airline management of security programs and systems. The FAA has increased requirements and oversight of security personnel (selection, training, and management) and equipment (weapons and explosives detectors), but has not yet addressed how security personnel and equipment perform as components of a system.

Screener Selection and Training

For years, the people who screened airline passengers and baggage for domestic flights generally received little training, low wages, and few benefits.[15] Consequently, alarming numbers of domestic screeners failed unannounced FAA tests (22 percent failure rate in 1988).[16] Since there has not been a severe domestic terrorist threat against aviation in the United States, these shortcomings have not resulted in life or property losses.[17]

In light of public pressure following the Lockerbie disaster and costly fines stermming from FAA inspections, the Air Transport Association (ATA) developed an extensive set of screener selection, training, and compensation standards. ATA pro-

[10] Ibid., p. 3.

[11] Ibid., p. 28.

[12] Ibid., p. 28.

[13] Under the FAA organizational structure in place in 1988 through 1990, the Office of Aviation Security was represented by the Executive Director for Regulatory Standards and Compliance, to whom it reported.

[14] Knowledge of aviation technology and operations is important to aircraft and airport security. For example, special characteristics of aviation, such as large volumes of people and luggage that must be screened quickly, drive the security system design and functions.

[15] However, airlines customarily have higher standards for security personnel working in international operations.

[16] Lynne Osmus, office of Aviation Security, FAA, personal communication, Feb. 22, 1991.

[17] Depending on the definition, the destruction of a PSA flight in 1987, caused by a disgruntled ex-employee who shot the flying crew in flight, @@t be considered a terrorist, as well as criminal, act. In this case, the ex-employee had an identification card with which he gained access to the aircraft, so screener training was not an issue.

posed that airlines (or their security contractors)[18] consider education and health criteria, the ability to speak English, and aptitude test results before hiring screeners, and that they offer competitive wages, benefits, and incentives and follow a comprehensive training curriculum. In March 1990, the ATA asked the FAA to adopt its proposal as requirements for all airlines. Based on this cooperative industry effort, the FAA has required some of these suggested upgrades in training measures for screeners. (Most U.S. airlines have adopted at least some of the ATA recommendations; the failure rate on random checks has since dropped significantly.)19 The FAA decided not to include selection and wage standards because such a change would require public comment (i.e., through the *Federal Register),* thereby calling attention to perceived or actual security weaknesses.

Management Practices and Human Performance

The FAA mandates certain positions in an airline's organizational structure, such as a security director for the airline and security coordinators at each airport, but airline management practices and philosophy usually fall outside the scope of FAA regulatory authority. In Safe *Skies for Tomorrow,*[20] OTA found that the effect of airline operating or management practices on airline safety, and changes in those practices, were rarely addressed in FAA safety analyses.[21] The FAA's Human Factors plan cites the influence of management "culture" on human performance as one area where basic research is needed.[22] If the organizational "climate" (i.e., working conditions, wages, management, organizational culture, etc.) does not allow an individual to perform at his or her peak, it may not matter how well he or she is trained or how well designed the technology is.[23] The ATA proposal for upgrading screener standards suggests giving screeners employee benefits common in many industries (vacation, holiday, medical) that contractors often don't receive); offering to contractors the advantages of airline employment (e.g., low-cost travel) and career opportunities to top performers; providing monetary rewards to those who detect test weapons and explosives (and even higher rewards to those who find the real thing); and increasing wages to at least the "local prevailing rate." For comparison, in Israel, screeners are paid at a level considered a "good" salary, far higher than minimum wage. In Switzerland, they are paid at the rate of about $lOper hour. In the United States, rates are often near minimum wage.

The United Airlines' approach to improving screener performance on all flights from selected airports delineates one set of management techniques (box 5-A). Another approach has been undertaken by American Airlines, although only for its international flights.[24] American treats its international screeners as part of the American team. They are hired as full-fledged airline employees, not employees of a contracted security agency, and enjoy the same salary levels and benefits that ticketing agents do. The educational level of entrants appears relatively high, with a few individuals having advanced degrees. There appears also to be a real opportunity for advancement within American Airlines, and not just in the security division. Before starting work, the entrants are brought to Dallas (from across the world; many screeners are hired from the countries in which they will be working) for 2 weeks of training at American's headquarters. The training includes emphasis on the screening questions as well as on what to look for on the x-ray screens. The screeners ask the standard questions as to who packed the baggage and whether anyone could have placed contraband in it. But they also ask general questions regarding destination and travel plans, somewhat akin to the lines of questioning performed by El Al. Indeed, American has used Israeli security consultants in designing their security system. The screeners look for a number of specific characteristics, which remain proprietary to the company. If too many of the characteristics match a passenger, the individual's baggage will receive much closer inspection. Screeners are ro-

[18] Most screening for domestic flights in the United States is conducted by security Contractors, nOtairline employees.

[19] Lynne Osmus, op. cit., footnote 16.

[20] U.S. Congress, Office of Technology Assessment, op. cit., footnote 7.

[21] Ibid., p. 88.

[22] U.S. Department of Transportation, Federal Aviation Administration op. Cit., footnote 9, p. 15.

[23] Ibid.

[24] SOURCE: Site visit t. Dallas Airport, December 1990, and Homer Boynton, Chief of Security, American Airlines, personal communication, December 1990.

tated between looking at x-ray screens and interviewing passengers.

Periodically, security systems are tested by contractors, who choose an American employee to play a terrorist. A specific scenario is given to this impostor, and the reaction of the security personnel is noted. If they do not perform their functions, they may be subject to severe discipline, including termination.

The result of the overall approach, using incentives and threat of discipline for negligence, appears to be a well-motivated and alert force.

Security Equipment

Currently, the FAA requires airlines to employ relatively few types of security equipment—primarily x-ray devices and metal detectors. The FAA established minimum performance standards for detecting weapons and explosives, and since these technologies are radiation-based, the FAA also requires that they meet Federal health and safety standards .25 There are no standards governing operator interaction with the equipment, such as the layout of controls and display symbology options. At the time the FAA established x-ray and metal detector requirements (early 1970s), it had little expertise in human factors. Moreover, these technologies were relatively simple compared with aircraft cockpit and ATC consoles that the FAA had to certify without objective human-factors criteria, making human-factors standards for security a relatively low priority. However, many behavioral experts argue that properly developed human-factors standards could improve system performance for aviation security as well as safety.

In recent years, the FAA has issued regulations for security technologies-computer-controlled access at airports and explosive detection systems—that are considerably more complex and have wider system implications than x rays and metal detectors. **As has been commonly the case whenever new technology is used to solve a problem, attention is focused on the positive aspects of the technology—how effective it is—without giving full consideration to possible new human-factors problems caused by the technology. The lack** of attention to man/machine human-factors and system operating issues is evidenced in the explosive detection system (EDS) regulations published in September 1989[26] and the subsequent performance of TNA, the only device to date that could meet the FAA standards. Beyond setting detection criteria, which are critical to the security system performance, the FAA also included requirements for throughput of the device (which is primarily an economics issue—see ch. 4) and a requirement for 100-percent automated detection decisionmaking. Several lines of reasoning could lead to a design goal of total automation, including lower operating costs over the long run

Box 5-A—UAL Hi-Tech Screening

United Airlines is focusing on management practices in its program, called Hi-Tech Screening, to improve the quality of pre-departure screening and the public perception of this highly visible function. Begun in 1987 at Chicago O'Hare and San Francisco Airports, the program incorporated many of the selection and incentive steps later recommended in the ATA proposal, and also attempted to integrate technology and people by reconfiguring the screening environment to make it more pleasant for screeners and passengers as well as to improve operations. Although wages are still low, successful workers have the opportunity to join the UAL organization, instead of working as contract security personnel. Improvements include direct communication links to supervisors for oversight and advice to screeners, layout designed to minimize passenger delays, and multiple cues to passengers that security measures are being taken in a professional reamer (security supervisor in an elevated booth, passengers see themselves on video monitors as they go through metal detectors, signs describing procedures are clear and concise). United believes that the program has been successful to date in increasing public awareness and employee morale and competence. At Chicago, the employee attrition rate dropped by half and weapon detections and FAA test scores increased significantly (79 percent detection rate on FAA weapons tests prior to Hi-Tech and 92 percent subsequently). United has also installed Hi-Tech Screening systems in Denver, Los Angeles, Seattle, and Washington Dunes, with plans for additional implementation in the future.

SOURCE: Site visit to O'Hare, April 1990, and Richard Davis, Operational Security, United Airlines, Jan. 3,1991.

[25]For example, x-ray systems used primarily for carry-on baggage must meet the standards set by the Food and Drug Administration.

[26]54 *Federal Register* 36938 (Sept. 5, 1989).

and possibly removing human error from the operating loop. However, it maybe useful, and sometimes vital, to keep the human in the operating/decision-making loop, especially if he or she must respond during emergency or unusual conditions. As has been shown so far in TNA tests, the false alarm rate is well above earlier goals and human intervention is required quite often. While automation, in the context of an EDS, is a useful tool, and total automation may be an understandable goal, **requiring 100 percent automated functions in an EDS is not justified at this time. The** EDS regulations provide an example of where input from a group such as the FAA's Human Factors Coordinating Committee could help flag potentially troublesome human-factors aspects of security regulations.

Passenger Profiling

In-depth questioning of all airline passengers and detailed examination of each of their personal belongings and baggage is impossible in a modern transportation system. Since most of the millions of passengers that fly on U.S. airlines each year pose no security risk, targeting security resources on the small number of passengers who exhibit some elements of the threat "profile" is one way to increase security without clogging transportation flows. profiling can be a valuable component of a transportation security system, providing an independent complement to hardware-based (and often more expensive) explosives and weapons detection technologies. Successful profiling depends on a large support system including comprehensive intelligence networks and threat analyses, information system technology to process large databases, behavioral research and analysis, and trained and motivated screening personnel.

There are two general approaches to operational profiling. One compares passenger demographic and other background data (age, sex, nationality, travel itinerary, etc.) to historic or recent intelligence-derived "threat profiles." The other is based on the examiner's psychological assessment of the passenger, taking into account nervousness, hostility, or other suspicious characteristics. Most profiling systems currently use elements of both approaches to varying degrees.

Airline passenger profiling, in most cases, must be fast (and consequently cursory) enough so as not to impose excessive delays. In other security contexts, such as screening for the "insider threat" profile within an organization where time is not so critical, much more detailed background data and questioning is possible. A different, although overlapping, form of profiling is used by law enforcement and investigatory agencies. Given pertinent data and evidence from a crime scene or threat, experts compile a profile of likely social, psychological, and physical characteristics of the criminal. However, much of the work and methodology could be transferred from one of the broad profiling regimes to the other.

FAA Requirements for Profiling-Under Federal regulations, U.S. airlines must apply a relatively simple form of passenger profiling for international flights (e.g., questions regarding electronic devices), although airlines are not prohibited by FAA/DOT from conducting any form of profiling at any time. Whether or not a passenger is selected for closer scrutiny, such as a manual baggage search, depends on where his passport was issued (a factor that varies based on threat intelligence) and on responses to a series of questions aimed at identifying potential terrorist "dupes." Additionally, airlines must conduct random baggage inspections on a small percentage of otherwise unselected passengers for each flight. These requirements do not apply to domestic flights or to foreign airlines, which results in an obvious gap in protection for Americans. **The fact that foreign airlines that compete with U.S. airlines on international routes do not have to satisfy these requirements imposes an economic penalty on domestic carriers and weakens their ability to compete successfully with foreign carriers, which, in addition, are usually state-subsidized. Domestic airlines complain, with justification, that a "level playing field" should be established to avoid this unfair disadvantage. An option would be to compensate** U.S. airlines for the additional costs, either from Federal subsidies or from the Airport Trust Fund.[27] Alternatively, foreign carriers could be required to apply similar security measures on flights landing in the United States to those demanded of U.S. carriers. The United States has forced better security practices in foreign

[27] In 1976, Congress established a precedent for compensating U.S. air carriers for security measures incurred in international operations by authorizing nearly $10 million for fiscal years 1976-78 (Public Law 94-353, sec. 24). In 1982, Congress extended the authorized limit to $15 million (Public Law 97-248, sec. 524(d). Nearly this much was actually disbursed to four U.S. carriers.

airports by threatening **revocation of landing rights of carriers from those countries in the absence of improvements.**

U.S. airlines operating on European routes have been permitted to substitute their own profiling programs for FAA requirements.[28] Most U.S. airlines and many foreign carriers conduct more extensive profile screening than minimum FAA requirements at foreign airports and some U.S. international gateways. Some airlines train their international employees in profiling techniques while others hire contractors to handle security for their international flights. Proprietary profiling procedures used by these airlines are modeled generally on the Israeli El Al method of profiling which is more comprehensive (and intrusive) than FAA requirements and reportedly includes psychological, social, and political factors. Complaints by certain groups, such as Arab-Americans, claiming harassment, stem from carrier-initiated profiling, not Federal requirements.[29]

During the past 5 years, the FAA has developed and tested a computer-based profiling tool aimed at potential terrorist hijackers and saboteurs. The Comprehensive Passenger Screening Profile (CPSP) is both a checklist and decision aid for field officers and a data collection system to support profiling enhancements. It encompasses the current FAA required profiling procedures plus additional factors based on a data profile of terrorists, using historical and intelligence sources.

The decision process for selecting a passenger for further examination is automated through a series of mathematically weighted yes/no questions (some of which do not require passenger interviews), that the security officer responds to via a keyboard. CPSP is designed for easy modication if intelligence or data analysis indicates a need. In early 1990, the FAA offered CPSP as an option for airlines to meet profiling requirements. Continental Airlines and United Airlines have tested versions of CPSP at a few locations, and have been generally pleased with its performance, especially as a tool for centrally coordinating security management decisions and for providing a conduit for a detailed database.[30]

The FAA is considering making CPSP mandatory, but a number of carriers oppose it, citing security officer vigilance problems caused by distraction by computer keyboard and display. Knowledgeable FAA and airline personnel claim that airline opposition stems mainly from the increased oversight capabilities that such a system would give the FAA CPSP would provide a detailed record of all airline profiling actions (and errors or failures) that could be used for civil penalty proceedings. Presently, the FAA oversees airline profiling procedures through random or scheduled field visits.

The FAA counters that if a would-be malefactor sneaks through, CPSP also can provide documented proof that the airline followed FAA-required procedures, shifting some liability for a profiling failure to the FAA.[31] **Additionally, there is substantial analytic value to the large data set that would come from CPSP.** As discovered during TNA testing, little is known about the baseline average passenger and baggage; therefore, general background data, regardless of how well CPSP works operationally, would be valuable for security planning. No names of passengers are (or legally can be) included in such a data set maintained by the Federal Government.[32] However, as private entities, airlines can and do maintain such lists.

Other Issues for Human Factors and Profiling

Research and Development

Due to security and proprietary concerns, profiling systems in place today are shrouded in secrecy. The technical aspects of their development and quantitative measures of their performance are difficult to obtain, although the widespread use at airports across the world attest to airline confidence in profiling Given industry acceptance of profiling technology, the unregulated environment in which profiling systems were developed, and the potential enhanced capabilities and future needs, there is a

[28] Leo Boivin, FAA Intelligence, personal communication Oct. 18, 1990.

[29] Ibid.

[30] John Beardslee, Director, Corporate Security, Continental Airlines, personal communication, Oct. 15, 1990 and Glen Winn, Director, Operational Security, United Airlines, personal communication, Oct. 16, 1990.

[31] Op. cit., footnote 27.

[32] Ibid.

role for a concerted Federal (DOT) effort in profiling R&D.

The primary research fields of interest are in the behavioral sciences and in large database collection and analysis. A useful but neglected approach would be to investigate the role of cultural differences in establishing profiles. Since patterns of behavior considered anomalous in one culture are normal in others, understanding cultural effects better could lead to more effective and, possibly, less discriminatory use of profiles.[33] Relevant behavioral research with applications for profiling is being conducted by a number of Federal agencies, although they generally do not coordinate these research efforts.

There is a need to coordinate research and experience in developing terrorist profiles among concerned agencies. Also, some work is going on to establish databases of past incidents and known terrorists in order to help develop profiles. The FAA conducts a modest profiling research effort that produced the CPSP and is analyzing profiling field tests. **However, this effort is housed in the intelligence section under the Assistant Administrator for Civil Aviation Security with no direct link to FAA's R&D division.**

Historically, the FAA pioneered the use of profiles in aviation in the late 1960s and early 1970s during the upsurge of hijackings to Cuba. A team of experts under the leadership of the FAA Office of Aviation Medicine was involved in the development of the initial profiles. Limited use of profiles was made during the early 1970s and again in 1980, when immigrants from the Mariel Boatlift began hijacking aircraft to Cuba. [Profiles were employed on a limited basis to help stem the wave of hijackings to Cuba by some "Marielitos".]

In the 1970s, the FAA also developed a profile for domestic use to identify persons who might be carrying explosives or incendiary devices in checked baggage. This "checked bag" profile included several objective elements and was intended for use by airline personnel at ticket counters. This profile was never applied rigorously, although some of its elements were automated by at least one U.S. air carrier.

Thus, the FAA has had substantial experience with developing and implementing profiles for use in aviation security. It has worked with in-house experts, with other agencies, and with behavioral scientists under contract. **There should be steps taken to guarantee that this institutional knowledge is not lost, due to needed secrecy or personnel turnover.**

There should also be an effort to bring together knowledge on profiling from the Intelligence Community, from the Federal Bureau of Investigation, from the Immigration and Naturalization Service, and from the FAA, so that all agencies may profitably pool their knowledge. One way of helping assure such interagency communication would be the institution of annual interagency conferences on the topic (see ch. 3).

Profiling techniques and related technologies are being added to current security R&D plans **at the** FAA Technical Center. The operational aspects of using automated profiling systems, such as data entry and human/computer interaction, are similar to those of many other technologies, and could benefit from further research and development.

A near-term research need is how best to combine profiling systems with the new security technologies now in the pipeline. In fact, arguments have been made that the TNA device can only function effectively when combined with profile-based selection of baggage to inspect, since false alarm rates are high. This is, in fact, being done at the Gatwick tests. Presently, the profiling process results in binary decisions—let the passenger pass into the normal security process (more than 95 percent of passengers) *or* conduct a manual search of the passenger and his baggage. **One possibility would be to expand and refine the decision outcome from profiling to provide multiple screening paths for passengers depending on the level of threat and the availability of advanced detection equipment (see ch. 4).**

A longer term research option is to investigate new technologies to enhance profiling. Rapid access in the field to Federal, international, and, possibly, private databases (i.e., hotel, credit card) could greatly enhance capabilities. Remote sensing of respiration and heart rates and other biological parameters, combined with large population databases, automated facial-recognition systems, and

[33] Customs officials in the Northern Mariana Islands, a U.S.-flag territory, incorporate cultural characteristics in looking for anomalies for profiling.

biometric passports, all offer new possibilities for on-the-spot psychological and physiological assessments.

Civil Liberties

Security systems in general, and profiling methods in particular, trade certain freedoms (e.g., privacy) for safety. profiling methods, based on specific individual characteristics, may be derived from historical experience (e.g., the large number of Cuban refugees who hijacked aircraft to Cuba in the early 1970s or the examples of hijacking engaged in by members of various Middle Eastern terrorist groups). These characteristics sometimes include physical and cultural features, since these traits are the easiest indicators to verify. Often such subjects belong to readily distinguishable minority groups. Therefore, people who possess the characteristics in question but who have no ill intentions (obviously, the great majority) could be subjected to scrutiny that could be considered to encroach on individual freedoms.

This study describes measures to meet compelling public safety interests. It is, however, beyond the scope of this study to discuss the many legal and societal civil liberties issues involved (e.g., how much intrusiveness on privacy is countenanced by a compelling interest of the state?). It is certain that the technical ability to investigate and record personal histories and characteristics and the demand for the use of such ability will greatly expand, thereby increasing the potential for crossing the fine line protecting constitutionally guaranteed individual liberties. Legislative attention will have to address the tradeoff between public safety and welfare and civil liberties.

Incident Management

Human factors also play a role in managing incidents abroad. When U.S. citizens are held hostage in a foreign country, the United States often plays a role in resolving the incident. Some foreign security officials are trained in the United States under assistance programs. But the United States also may participate actively, as it did in responding to a number of airline hijackings in the 1980s.

From past experience, cultural factors particular to the country where the event is taking place frequently influence decisionmaking by local authorities. Some observers report that U.S. officials who were involved would, on occasion, have benefited by a more detailed knowledge of the dynamics of local social systems. For example, in some cases, although crisis management officials were supposed to be in charge of handling an incident, local cultural or political factors have resulted in the crisis being directed instead by senior office holders, who are untrained for the purpose and unable to provide the rapid decisionmaking that is often required.

Some research into systematizing knowledge of relevant aspects of different social systems would be useful. In this area, as in profiling, the construction of appropriate databases would be of use to U.S. officials who may be called on to participate in resolving a crisis. At present, there appears to be little coordination among agencies in understanding behavioral aspects of incident management. This lack provides another argument for strengthening interagency coordination in counterterrorism (see ch. 3).

Policy Options

The following policy options address human factors and aviation security.

1. Enhance FAA attention to human factors in security:[34]
   - Explicitly address aviation security in agency-wide human-factors planning.

     The FAA has taken measures to move in this direction.
   - Bolster human-factors expertise under the Assistant Administrator for Civil Aviation Security and the Aviation Security Research and Development Service at the FAA Technical Center by adding professionals to their respective staffs, especially in light of plans to increase staff levels of both sections significantly during the next few years. One such professional has already been added.

[34] The following recommendation, included in earlier drafts of this report, has already been implemented by the FAA
• Add a designee of the Assistant Administrator for Civil Aviation Security to the FAA's Human Factors Coordinating Committee.

2. Consider conducting R&D on combining passenger profiling techniques with other security technologies.
3. Give consideration to methods for "leveling the playing field" when imposing requirements on U.S. carriers but not on competing foreign ones.
4. Give consideration to civil liberties issues stemming from Federal aviation security requirements.
5. Coordinate behavioral research into profiling and incident management being conducted in the Federal Government. Arrange periodic interagency conferences on related topics.