

Phase I Report by a Panel of the

**NATIONAL ACADEMY OF
PUBLIC ADMINISTRATION**

*for the American Association of Airport Executives
and Airports Council International - North America*

ENHANCING AIRPORT SECURITY
Phase I Report

December 2000

Panel

Alan L. Dean, *Panel Chair*

David O. Cooke

Michael E. Levine

Len Limmer

Richard Monteilh

Philip A. Odeen

Cindy Williams

Officers of the Academy

David S. C. Chu, *Chair of the Board*

Jane G. Pisano, *Vice Chair*

Robert J. O’Neill, Jr., *President*

Philip J. Rutledge, *Secretary*

Sylvester Murray, *Treasurer*

Project Staff

J. William Gadsby, *Director, Management Studies*

Arnold E. Donahue, *Project Director*

Kenneth F. Ryder, *Senior Consultant*

Joe P. Mitchell, *Research Assistant*

Matthew A. Lewis, *Research Assistant*

Martha S. Ditmeyer, *Project Assistant*

The views expressed in this document are those of the panel alone. They do not necessarily reflect the views of the Academy as an institution.

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND	2
The Federal Aviation Administration.....	2
Aviation Security: A Tripartite Relationship	2
Evolution of Current Structure and Arrangements	5
Major Aviation Security Standards and Requirements	6
Comprehensive Inspections and Compliance Testing.....	10
ASSESSMENT	12
The Status of the FAA, Airport, and Airline Relationship.....	12
Security Practices	16
Addressing Public and Political Perceptions	17
RECOMMENDED AREAS OF STUDY FOR PHASE II	18
APPENDIX A: PANEL and STAFF	21

ENHANCING AIRPORT SECURITY

Phase I Report

INTRODUCTION

The American Association of Airport Executives (AAAE) and Airports Council International - North America (ACI-NA)¹ asked the Academy to examine the regulatory model that governs security relationships between the Federal Aviation Administration (FAA) and airport authorities. They raised concerns about the current status of relations among the security partners and wanted the Academy to consider ways of improving the operation of existing security procedures, practices, and relationships and possible alternative models or approaches that might enhance airport security. This report reflects the results of the preliminary phase that focused on:

- Identifying (1) the objectives of airport security within the totality of air passenger and aircraft security, (2) how the current FAA regulatory model came to be and is applied, and (3) the basis for the airport security standards, including the physical, technical, personnel and information security regulations.
- Examining the relationship between airport security and the other important elements of air passenger and aircraft security. This would include (1) the regulation of air carrier and indirect air carrier security, (2) the law enforcement community—international, federal state and local, and (3) the warning and alert responsibilities of federal and local entities.
- Initiating a preliminary exploration of (1) potential improvements to the current regulatory practices, both substantive and procedural, and (2) alternative models that might enhance the prospects of meeting the security objectives of the airports, air carriers, and passengers.

This Phase I report by the Academy's Panel on Airport Security identifies critical problems and/or opportunities that will serve as the basis for more detailed, follow-on assessments of agreed upon issues. The follow-on Phase II review will involve a more intensive examination of selected areas, leading to specific recommendations to improve aviation security.

¹ Several airport authorities, including Dallas Fort Worth International Airport, Houston Airport System Metropolitan Washington Airport Authority, Minneapolis -St. Paul International Airport, Seattle-Tacoma International Airport, and The Port Authority of New York & New Jersey, directly contributed toward this study and production of this report.

BACKGROUND

THE FEDERAL AVIATION ADMINISTRATION (FAA)

The FAA is the operating administration under the Department of Transportation (DOT) responsible for aviation operations, safety, and security. Its major functions are:

- First, it operates and maintains a network of airport traffic control towers, en route control centers, navigation aids, and flight service stations to allocate the use of airspace under air traffic rules and regulations it develops and promulgates. The safe and efficient utilization of airspace is a primary objective. FAA is engaged in a massive modernization of its air traffic control system to replace obsolete equipment and to handle an ever-increasing volume of air traffic. Increasing flight delays and airport traffic congestion have received priority attention during the last year from Congress, the Secretary of Transportation, the FAA Administrator, and airline executives.
- Second, FAA issues and enforces rules, regulations, and minimum standards relating to the manufacture, operation, and maintenance of aircraft, the rating and certification of airmen, and the certification of airports serving commercial air carriers - functions closely tied to the safety of civil aviation. Commercial aircraft maintenance and repair has also received increased FAA emphasis as a result of several recent commercial aviation accidents associated with aircraft maintenance deficiencies.
- Third, it manages the nation's civil aviation security program to prevent or deter terrorism and other unlawful interference with civil aviation. Concerns about aviation security have grown rapidly since the early 1960s, and these are periodically re-emphasized after major terrorism incidents.
- Finally, FAA supports airport planning, development, and improvements to meet capacity needs, to reduce airport noise, and to improve safety and security.

Virtually all FAA activities directly involve aircraft manufacturers, commercial airlines, general aviation, and/or the nation's airports, thus requiring considerable coordination and extensive interaction in order for the FAA to accomplish its missions.

AVIATION SECURITY: A TRIPARTITE RELATIONSHIP

The nation's civil aviation security program is a system of shared and complementary responsibilities among three principal elements. The FAA provides threat information, establishes aviation security policies and regulations, evaluates the effectiveness of airport and airline security activities, and provides funding support for some of these activities. Approximately 450 commercial airports are responsible for providing a secure ground environment, which includes a local law enforcement presence at their facilities and only authorized access to secure areas of the airports. Finally, the nation's commercial airlines, more than 100 of them, have the principal responsibilities for the security of their aircraft and for screening passengers, baggage, and other cargo for weapons and explosives.

In more detail, the roles, responsibilities, and missions of these three entities are:

- **The FAA's Civil Aviation Security (ACS) office:** The ACS has three components servicing its three major functions:
 - Its intelligence office analyzes threat information to civil aviation - primarily foreign and domestic terrorism, but also other illegal interference. It provides FAA field personnel, airports, and airlines information circulars on the nature of the aviation security threat and, occasionally, warnings of specific terrorist and other threats. The FAA, however, has no unilateral intelligence collection capabilities; it relies on the intelligence community for foreign terrorism information, and on the FBI to acquire domestic intelligence and to help with airport threat and vulnerability assessments. Airports also receive intelligence support directly from local FBI field offices and other local law enforcement agencies, and local law enforcement councils at airports often serve as liaison to exchange information on potential threats and criminal trends.
 - ACS' policy and planning office develops aviation security policies and regulations. It is responsible for the major FAA regulatory policies, including Federal Aviation Regulations (FARs) Nos. 107, 108, 109, and 129 that address, respectively, airports, U. S. air carriers, indirect air carriers, and foreign air carriers. This office also issues mandatory changes to airport and airline security plans, required by regulation, through emergency amendments and security directives.
 - ACS' operations office approves the individual airport and airline security plans, monitors compliance, and initiates enforcement in case of violations. ACS Operations is the largest of the three ACS offices. It includes federal security managers at 19 major (Cat X) airports who are directly subordinate to ACS headquarters and the FAA's nine regional security divisions with their subordinate civil aviation security field offices (CASFOs) and field units (CASFUs). These local offices and units are usually located at or near the country's major airports, and inspectors, generally special agents, in these components conduct periodic comprehensive inspections and ad hoc special emphasis assessments to judge regulatory compliance. In addition, these inspectors are responsible for enforcement actions and investigative reports that serve as the basis for corrective action and/or civil monetary penalties for violations.

These three major ACS offices also carry out the FAA's security-related responsibilities and regulations for hazardous goods and cargo and serve as a resource to support law enforcement agencies involved in drug enforcement activities, although the FAA and screeners have no operational role in these activities.

These offices also work with other FAA components that have major roles in the areas of developing and acquiring technical security equipment (Research and Acquisition), funding airport improvements (Airports), and overseeing both airport and airline safety (Regulation and Certification). In conjunction with the nation's

airports and airlines, ACS works with these other FAA components to guide development, acquisition, construction, and training activities related to aviation security.

- **The airports:** The nation's airports that service scheduled passengers and certified air carriers are the venues where most aviation security activities occur. The airport's management includes an airport security coordinator and other security components, such as an airport police force with full law enforcement authority (sometimes augmented by local and/or state police) and an employee clearance and badging office. These are responsible for the physical security of airport facilities, law enforcement, and personnel security. Airport management attention is more broadly focused on the total security of airport facilities in contrast to the FAA's narrower emphasis on securing aircraft from acts of terror or unlawful interference. This is reflected in the FAA's security regulations which specifically require that airports:
 - Submit and maintain, subject to FAA approval, an airport security plan that restricts access to aircraft and air operations areas. (Most of these plans are on the order of several hundred pages and require frequent amendments for structural modifications and operational changes, such as closing or sealing doors, adding or changing concessionaires, etc.)
 - Maintain on-site law enforcement capabilities with arrest authority to respond to incidents, threats, or interference.
 - Badge personnel, specifically cleared according to FAA criteria, for unescorted access into designated airport areas.
 - Specify the air operations areas restricted to cleared, badged personnel and maintain access control to these areas.

There are numerous derivative airport security requirements incorporated in regulations or plans that specify, for example, the response time of law enforcement personnel under varying circumstances, the integrity of badging systems, the length of time access doors may be opened for passengers, etc. Record keeping requirements on cleared personnel's employment history and on the date and time of personnel accesses are also specified in regulations.

- **The passenger airlines and indirect (cargo) air carriers:** While the airports are the venue for the bulk of airport security operation, the airlines and other air carriers are responsible for implementing those security activities that directly affect the flow of passengers, baggage, and cargo aboard aircraft. FAA regulations require airlines to:
 - Submit and maintain, subject to FAA approval, an airline security plan, though there is an air carrier standard security plan about two hundred pages in length used by most airlines.
 - Screen passengers and carry-on luggage. Most of these activities are contracted out to security firms specializing in airport security operations.
 - Screen checked baggage and air cargo under procedures in its approved security plan. For most flights, a portion of checked baggage, based on passenger

- profiling, is selected and subject to screening or bag-matching to ensure that passengers accompany checked baggage.
- Clear employees and contract personnel with access to air operations areas based on the same FAA-specified clearance criteria used to clear airport personnel.

Under exclusive-use agreements for specified airport areas, airports may relinquish, and airlines may assume, responsibilities for issuing badges and controlling access for specified airport areas. As in the case of airport security, there are derivative requirements both substantive and procedural addressing airline security. These include such matters as passenger interrogation, maintenance of the integrity of screened passengers and baggage, employment history verification, and response guidelines.

EVOLUTION OF CURRENT STRUCTURE AND ARRANGEMENTS

Current aviation security policies, requirements, and practices have evolved since the early 1960s, heavily influenced by a series of high profile aviation security incidents. The key statutory and historical developments were:

- **The Air Transportation Security Act of 1974:** In response to a rash of aircraft hijackings, FAA established the air marshals program in the 1960s under the FAA's general regulatory authority to promote flight safety. In 1974, however the basic elements of the FAA's current aviation security program were incorporated into an Air Transportation Security Act, which specified:
 - FAA's authority to issue airport and airline security regulations, including unilateral mandatory directives, and to enforce compliance through civil penalties.
 - A requirement for airport law enforcement authorities.
 - Prohibitions on carrying weapons and explosives aboard aircraft
 - Requirements for passenger and baggage screening

During this period and up until 1990, the FAA's policy, regulatory, and enforcement authorities resided in the Associate Administrator for Regulation and Certification, who was also responsible for airport and aircraft safety.

- **The Air Security Improvement Act of 1990:** This 1990 act was passed in the aftermath of the 1988 Pan Am 103 tragedy and the report of the White House Commission on Aviation Security and Terrorism. It:
 - Elevated the FAA security organization to the level of Associate Administrator.
 - Directed that FAA security officials be stationed at major US and foreign airports; this became the basis for federal security managers at 19 major US

airports and foreign liaison officers at 20 major foreign airports serving foreign and domestic air carriers that fly to the US.

- Mandated employment history and limited background-type checks of personnel with access to aircraft.
- **The Federal Aviation Reauthorization Act of 1996:** This 1996 act was passed to reflect the initial recommendations of the Presidential Commission on Aviation Safety and Security, sometimes called the Gore Commission. This Commission was established in response to the ValuJet and the TWA 800 crashes earlier that year, and focused heavily on aviation security concerns. Ultimately, neither crash was found to relate to security. This 1996 act's provisions:
 - Encouraged FAA to acquire and deploy the technical equipment recommended by the Commission
 - Expanded the number of employees subject to background checks to include baggage and passenger screeners
 - Directed FAA to certify screening companies
 - Increased the number of FAA security employees to audit background investigations and to conduct regular, unannounced airport security investigations
- **The Airport Security Improvement Act of 2000:** As this report was in final preparation in late October, this statute was enacted on a bipartisan basis to address concerns about aviation security, partly in response to recent complaints about security at airports. Its major provisions:
 - Require the FAA to work with the Office of Personnel Management and the Federal Bureau of Investigation to implement criminal history background checks of prospective cleared employees through electronic fingerprint transmission and expands the list of disqualifying offenses
 - Specify training standards for screeners and requires FAA to expedite its rulemaking on screening company certification
 - Require airport and air carrier operators to implement a program of progressive disciplinary penalties against employees, under FAA guidelines, for infractions against airport access controls.

These new provisions of law have not yet been implemented, but the net effect is to require greater direct FAA involvement in background checks, screening operations, and access control programs.

MAJOR AVIATION SECURITY STANDARDS AND REQUIREMENTS

The nation's aviation security program rests on four major regulatory pillars:

1. Screening of passengers and carry-on luggage for weapons and/or explosives

It is illegal for passengers to carry weapons or explosives aboard a commercial airliner. To deter this, passengers are screened through magnetometers to prevent entry with weapons, and carry-on luggage is x-rayed for indications of weapons or explosives. This usually takes place at concourse or gate checkpoints. Carry-on luggage may also be subjected to explosive trace detection systems that can detect explosive particles or residue on the external surface of the luggage. Although there are numerous special circumstances when screening is performed, all commercial flights with seating for more than 60 passengers are required to conduct passenger and carry-on screening, as well as flights bound for connections at secure airport areas where there will be no further screening.

There is widespread concern that screening operations are less than fully effective because of the capabilities of personnel deployed for this task. Most screener positions are paid close to, or at, minimum wage and experience high turnover. FAA has two major programs underway to address these concerns:

- Deployment of x-rays capable of threat image projection (TIP) that can be used to enhance screeners' concentration, accustom screeners to new weapon and or explosive configurations, and test screeners' skills.
- Certification of screening companies, as required under the 1996 reauthorization act and the most recent Aviation Security Improvement Act. FAA has prepared a draft regulation covering screening company certification that is tied to the introduction of TIP-ready x-ray equipment. Though FAA has not had responsibility for the certification, training, or re-training of individual screeners to date, the new 2000 law requires FAA to establish minimum standards for screener training.

Currently, about 2,000 weapons are seized annually at passenger screening checkpoints. While most incidents of weapons carriage are benign in intent, about 1,000 persons are arrested annually, either for weapons carriage or for making false statements about weapons.

2. Screening of checked baggage and cargo for explosives

Baggage and cargo screening are currently tied to passenger and cargo profiles, computer-assisted at larger airlines or manual ones by counter personnel or skycaps. These profiles are generally tied to elements that might indicate a greater likelihood of a terrorist or other incident. The Department of Justice has reviewed these profiles and determined that they are not biased and do not violate an individual's freedoms. On international flights, suspect baggage is screened by explosive detection systems (EDS), explosive trace detection (ETD) systems, and/or canines or subject to bag-matching that assures passengers accompany checked baggage. FAA information on the extent and success of baggage screening operations is closely held and not readily available.

In addition, FAA has major programs underway to develop advanced systems better able to detect explosives, lower cost and weight units for smaller airports, and units with a greater throughput. It is acquiring additional explosive detection units as funding permits with a long-range goal of eventually achieving 100% baggage screening, both internationally and domestically.

3. Controlling access to secure air operations areas

While passengers and their baggage are considered the most likely means of introducing weapons or explosives aboard commercial aircraft, FAA regulations attempt to prevent other means of introducing explosives aboard or otherwise endangering aircraft integrity by requiring airports to control access to air operations areas. Unescorted personnel must be properly badged, the badge must be openly displayed, and operations area personnel are expected to challenge persons not displaying a badge. In addition, access control systems record badged employees' accesses by date and time. Most large airports have access rosters well into the tens of thousands, and a very large number, often hundreds, of entrances for baggage handlers, aircraft and facility maintenance personnel, construction workers, cargo facilities employees, fueling operations personnel, caterers, and cleaners.

Controlling access to air operations areas has proved extremely difficult. A DOT Inspector General test of airport access controls in early 1999 demonstrated that piggybacking through access controlled entries and other techniques was exceedingly easy, achieving unauthorized access in 68 percent of the attempts. In addition, access to aircraft, including aircraft interiors, by unbadged personnel went unchallenged. This resulted in considerable adverse publicity and seems to have generated an intensive FAA compliance testing program, as well as more aggressive airport and airline programs to curtail piggybacking and other access control violations. For example, the number of access doors has been curtailed, but fire doors, required by airport safety regulations, remain a difficult and contentious point of vulnerability since they cannot be secured. Airports have also increased employee rewards for challenging unbadged personnel and/or employee penalties for failure to display badges. As a result, the incidence of operations area and aircraft penetration appears to have been significantly reduced. The recent Aviation Security Improvement Act endorses programs to increase individual accountability and now directs FAA to cooperate in their enforcement by requiring FAA to provide guidelines for the type of penalty programs now in effect at many airports. For airports, this has the effect of placing more emphasis for access controls on individual airport and airline employees, allowing airport security to increase security focus on the entire airport facility. Greater federal emphasis on infrastructure protection has heightened concern about the vulnerabilities of airport terminals, their fuel stores, and other airport facilities, requiring increased surveillance beyond the aircraft themselves for potential threats from weapons or explosives.

FAA regulations treat airports and airlines, not individuals, as the regulated parties accountable for violations. Airports have encouraged FAA to adopt a system of

individual accountability that would make airport and airline personnel directly accountable for failure to display badges or challenge unbadged personnel. This would allow airports to give greater attention to protecting other customers and their physical facilities, not just aircraft and their passengers. Air carriers are concerned that individual accountability rules may divert the attention of their personnel from dangerous and/or critical flight preparation tasks. The FAA circulated a draft regulation on individual accountability earlier this year, and reportedly will issue a final regulation next year.

4. Clearing and badging personnel with access to secure airport areas and aircraft

The backgrounds of personnel requiring badges must be checked, based on rules prescribed in the Air Security Improvement Act of 1990 as amended and reflected in FAA regulations. Basically, these rules call for confirmation of employment history for the last ten years, with any employment gap longer than one year subject to a FBI criminal record check for a specified list of crimes that often carry penalties of incarceration of a year or longer.

DOT's Inspector General has questioned the validity of these criteria, contending that a large number of felons receive little or no incarceration and that significant felonies, such as burglary, larceny, etc., do not preclude badging and, therefore, access to secure operations areas of an airport. There is a concern that convicted felons, possibly unwittingly, may be enticed to introduce explosives aboard aircraft. AAAE and ACI-NA and most airports and airlines supported legislation that would require fingerprinting of all personnel requesting access to be used in a mandatory FBI criminal history check, as reflected in the recent Aviation Security Improvement Act.

There are numerous supporting and ancillary standards and requirements associated with these four major security pillars. For example,

- Most airfields are enclosed by a fence of specified height for both safety and security reasons. Natural barriers, such as the Potomac River at Reagan National Airport in Washington, DC, can substitute for constructed ones and are considered a sufficient deterrent. Perimeter barriers, including fencing and natural barriers, are not alarmed, and a determined intruder could, with varying degrees of effort, penetrate secure airport areas.
- Weapons carriage aboard aircraft by certain law enforcement officials is permitted, but subject to a separate check of the official's credentials and/or identification. This policy recently received high-level review when GAO personnel, masquerading as police officers with fake identification, avoided screening and penetrated government office buildings and a few airports. As a result, FAA raised the bar and required that airport police, not just checkpoint supervisors, approve unscreened access by law enforcement officers.
- FAA regulations require airports and airlines to account for badges and to re-issue all badges if more than 5 percent are unaccounted for. Because of temporary badging for maintenance activities or construction projects and because of the huge turnover in

low paying cleaning and screening positions, airports and airlines have developed innovative ways, such as monetary rewards, to encourage badge returns and avoid the heavy expense of re-badging personnel.

COMPREHENSIVE INSPECTIONS AND COMPLIANCE TESTING

The FAA, operating through its nine regions and their subordinate units, has had a long-standing program of comprehensive inspections of airports and airlines for safety and security. These included in-depth, annual, announced examinations of all the larger airports (Cat X and Cat 1), including the commercial airlines and cargo carriers at these airports. Periodic, but less frequent, examinations of other airports and air carriers were also conducted. These comprehensive inspections focused on safety and security processes and procedures that the airports and airlines used to implement safety requirements and their FAA-approved security plans. Safety inspections, required under FAA Regulation 139, are pre-planned, structured, and done cooperatively with airport staff, often part of the same staff responsible for security. These comprehensive safety inspections covered most aspects of safety activities and provided both the FAA and the airports or airlines opportunities to identify weaknesses and assess approaches for addressing them. Up until recently, airport security have been generally similar - announced, process-oriented, and cooperatively conducted with airport security staff. But, they also included some limited testing of the actual implementation of specific procedures of, for example, access controls, audits of background checks on employees, and badging operations.

In addition, FAA inspectors would supplement these periodic, announced comprehensive inspections with unannounced spot inspections. FAA regions and field offices had considerable discretion regarding the frequency and focus of these supplemental inspections and the use of the results and findings. The effectiveness of the comprehensive inspections supplemented by discretionary spot inspections was questioned by some FAA staff and outside observers. In particular, DOT's IG found these nominally comprehensive inspections seldom complete and often unsatisfactory.

In late 1999, ACS' Operations office switched to almost complete reliance on a centrally-designed and headquarters-controlled program of rigorous compliance testing of specific airport and airline security features. It curtailed comprehensive assessments except in cases of new airline operating locations or major security modifications at existing airports. In contrast to the previous announced comprehensive assessments with occasional spot inspections, the compliance testing the FAA has recently conducted has been unannounced, tightly controlled, and more consistently applied in all regions. Each inspector's actions were closely controlled by strict protocols, developed by Washington-based staff, with little regional discretion on the timing and targets of the tests. Some airports and airlines seem to believe that these recent tests are not focused on significant security vulnerabilities, but rather on known weaknesses. In their view, some of these weaknesses are not significant security vulnerabilities, some are not easily correctable, and some are weaknesses in areas where they have been attempting to correct the human

factors and/or equipment deficiencies that contribute to security violations. Finally, airport and airline security personnel seemed to be poorly informed about the results of these tests, particularly the measures ACS was using to determine trends and comparative performance.

This more aggressive, recent FAA compliance testing program has been accompanied by a much more rigorous and standardized treatment of alleged violations and imposition of civil penalties. During the current compliance testing, inspectors have been required to write investigative reports, cite violations, and have little or no discretion to take into account the severity or circumstances of the incident. This seems to have been in marked contrast to the inspector's past practice of issuing warnings to airports or airlines of potential violations, giving these organizations an opportunity to correct deficiencies before formal investigative reporting.

Once violation reports are drafted, the offending airport or airline is given an opportunity to comment on the report, cite mitigating circumstances, and offer corrective actions it is taking to ameliorate or prevent re-occurrences. CASFU and, sometimes, CASFO supervisors are given the opportunity to consider circumstances and corrective actions in recommending judicial action and/or the amount of penalty. These range up to \$11,000 per incident for airlines and up to \$1,100 for airports. The FAA regions may also review inspectors' investigative reports, but these reviews appear to consist of a technical review to ensure that the violation has been well documented. Finally, the regional counsel is tasked with reviewing case files, conducting informal hearings, and determining penalties, subject to a full administrative law judge hearing upon appeal. Violations may also be aggregated into a single penalty by the regional counsel, and extremely large penalty awards are often forwarded to FAA headquarters for review and approval. Most airports report that they generally attempt to address violations locally, with the federal security manager in the case of Cat X airports or with their local investigating unit (CASFU), but seldom will address appeals beyond the local level.

Individual airports and airlines often conduct self-inspections to determine the effectiveness of their security activities, sometimes duplicating the FAA's compliance testing programs. These airport and airline self-inspections include daily badge-check and challenge activities by security personnel, airport reward programs for identifying unbadged personnel in secure areas, penalty programs for improper badge display, and testing of access control, baggage screening/matching activities, passenger screening, and tests of law enforcement response times to alarms and incidents. These programs tend to emphasize an employee's individual accountability for his/her own actions. Though it was not possible to determine the historical patterns and trends in these activities, they appear to be extensive. Some interviewees contended that self-inspection was necessary to accurately assess their own security performance because FAA inspections and tests were unreliable and that, in any case, the detailed results were unavailable.

In addition, the airports and airlines rarely share the details and results of their own inspection and testing activities with FAA. A frequently cited reason for not sharing these data on vulnerabilities and test results was that these would then become the basis

for additional FAA testing, leading to violation citations and civil monetary penalties. Many airports, in particular, cited unpleasant experiences when airport consortia conducted vulnerability assessments in response to a Gore Commission recommendation. These consortia, set up at many major airports and composed of airport, airline, and FAA personnel, identified deficiencies and developed corrective security action plans. Airport and airline personnel feel that the deficiencies they acknowledged in this process were used to guide FAA enforcement actions despite a promise of immunity.

ASSESSMENT

The background information above is selective and does not attempt to provide a comprehensive description of the development and complexity of aviation security. Rather, it was chosen to help illuminate the key areas where the Panel has focused its assessment and there seem to be major opportunities to enhance aviation security. These include:

- the status of the tripartite FAA, airport, and airline relationship
- the best practices for aviation security
- public and political perceptions of aviation security

The selection of these three areas for assessment is not meant to suggest that there are no other areas for possible further review and study, but the panel believes these areas are fundamental to significant improvements.

The Status of the FAA, Airport, and Airline Relationship

The current status of the relationship among the three aviation security partners is bent, but not broken. It seems to be badly strained, and complaints and criticisms from all three major partners provide evidence of growing tensions. Nonetheless, there is considerable cooperation and coordination at many levels, evidenced by regular meetings, information exchanges, and consultations. Indeed, when there is a real-world security crisis, cooperation improves noticeably and most problems disappear.

The major causes of the growing tensions among the security partners seem to be:

- **FAA Regulatory Policies:** The FAA's two major aviation security regulations (FARs 107 & 108) have been under revision for over a decade, and both airport and airline representatives expressed considerable unease with the uncertainties associated with these pending regulations. Current regulatory procedures preclude active dialogue with regulated parties during the final rulemaking review process to avoid the appearance of, and lessen the opportunity for, favoritism. There is a long-established Airport Security Advisory Committee (ASAC), composed of airport, airline, and ACS representatives, that serves as a federal advisory committee with twice yearly public meetings. But, sensitivity about security among the participants and the participation of unions, victim groups, and outsiders apparently limits the usefulness

of the ASAC. Outside Washington, both FAA regional and local personnel, as well as airport and airline personnel, felt little participation in, and ownership of, the regulatory process. The difficulty of meaningful participation and the extremely long period that these regulatory revisions have been under development appear to have undermined the credibility of the regulatory process and the industry's goodwill toward it.

FAA has sought to allay concerns about the FAR 107 & 108 revisions by indicating that the proposed changes are not significant, but both the airports and the airlines demonstrated considerable uneasiness about the possible outcomes. This anxiety appears to be compounded by an extensive list of other regulatory actions that the FAA has either proposed or has under consideration. These include regulations related to computer-assisted passenger-profiling systems, explosive detection and trace detection systems, individual accountability, screening company certification, and compliance programs. There is not unanimity among FAA, airports, and airlines on many of the issues inherent to these regulations, and this appears to have caused considerable anxiety among the aviation security partners. Another frustration broadly shared among all the partners is the long lead time needed to develop, review, and implement FAA security regulations. FAA headquarters personnel recognized and shared this frustration with the regulatory process as well, but contended that it was necessary to plan on a minimum of three years for a new security regulation to emerge.

The considerable uncertainty regarding the interpretation and meaning of existing regulations compounds the frustrations with the delays in and lack of inputs into the FAA regulatory process for aviation security. FAA regulations in aviation security seem to lack clarity and simplicity, a condition exacerbated by the variety of operating environments and circumstances to which these regulations apply and the protection of sensitive security-related information. Some airports seem to be opting for less specific and more generic security plans. These plans, intended to be a major vehicle through which regulatory requirements are particularized for different operating environments, are increasingly being limited to the bare essentials, eliminating provisions not explicitly required by FAA regulation. Such a development, extended to multiple airports and/or airlines, is likely to further strain basic relationships since FAA inspectors look to the plans to help define those circumstances or locations where regulatory restrictions apply.

Finally, there were repeated complaints about the numerous revisions to security plans through periodic amendments, security directives, and emergency amendments. The lack of timeliness in the FAA's normal regulatory system may have induced ACS to use, perhaps overuse, these more unilateral and less participatory regulatory processes to develop and implement specific security policies. FAA field and airport and airline security personnel felt they had little involvement in developing these security directives and emergency amendments, frequently referred to as "the Friday 5 PM faxes." The lack of field and industry inputs to these directives resulted in frequent revisions, yielding multiple revisions in response to implementation

difficulties. This, in turn, tended to further compound extant field interpretation problems. Some interviewees questioned the validity of FAA cost-benefit calculations for security regulations in general, and felt that the FAA systematically underestimated airport and airline costs. As passenger loads increase, they argue, these costs could escalate rapidly in terms of flight delays and passenger inconvenience and the security costs need to be traded off against system efficiency and safety considerations. Some also felt FAA used their directive authorities to avoid potentially unfavorable cost-benefit considerations prior to establishing a new policy. Weaknesses in threat information were also seen to debase risk-based cost-benefit calculations.

In its comments on a draft of this report, The Acting Administrator for Civil Aviation Security noted that the FAA regulatory process was constrained by the many different acts and executive orders governing the process and congressional limitations on the number of specialist that support rulemaking. He questioned the usefulness of further study, citing the mid-summer DOT Inspector General study of DOT's rulemaking process and a pending GAO audit of FAA rulemaking. These, he believed, confirmed the limits on the speed of the regulatory process and the degree of industry involvement. In addition, he felt there was an inherent trade-off between additional cost-benefit analysis and the time required to complete rulemaking.

- **Inspections and compliance testing:** The comparatively recent de-emphasis of comprehensive inspections and the substitution of rigorous compliance testing and enforcement have clearly contributed to the tension and strain among the aviation security partners. The larger airports seem to have experienced increased testing and scrutiny; they feel they have been singled out in an industry environment where seamless and, therefore, more uniform security treatment seems merited. Conversely, smaller airports have received less testing emphasis and sense that inspectors are neglecting comprehensive inspections they feel are more worthwhile.

While ACS and other aviation security personnel repeatedly cite the need to act as both "the cop" and "the coach" to improve security, industry representatives clearly feel the "cop" role is now substantially over-emphasized. The virtual suspension of comprehensive inspections and the increased reliance on compliance testing and enforcement clearly seems to have exacerbated the airports' and airlines' concerns. Both airport and airline representatives appear to feel the process of investigation, adjudication, and imposition of civil penalties detracts from their relationship with FAA, and contributes little to aviation security. Delays of 18 to 24 months in final settlement apparently are common. Although lengthy legal delays do not rest solely at the door of the FAA, numerous interviewees felt that the length of time for final administrative judicial action makes civil penalties lose all meaning with respect to correcting deficiencies and improving security.

The balance between comprehensive inspections and compliance testing is not easy to define, and clearly FAA relies much more heavily on FAA-approved and monitored self-inspections in the areas of airport certification and safety, airline maintenance,

and aircraft manufacturing. While the vigorous testing and enforcement protocols used by FAA's security inspectors has caught the attention of the industry, the industry feels this approach is inconsistent with FAA's practices in areas of potential vulnerabilities at least as severe as those associated with aviation security. While all partners acknowledge the value of rigorous compliance testing, the industry fears repeated bouts of intensive testing triggered by bureaucratic pressures and political reactions to aviation incidents. The airports and airlines might better perform some of the inspection and testing activities, with the FAA field inspectors auditing the processes and results. In the long run, however, a better balance between the enforcement and coaching roles of the ACS inspectors and a complementary mix of ACS, airport, and airline testing seem attainable.

- **Intelligence and Threat Information:** The paucity of information and intelligence concerning the magnitude and character of the threat is a common complaint of both the airports and airlines. In response to a Gore Commission recommendation, the FAA has cleared approximately 300 airport and airline personnel for classified information. But most have no classified communications and storage capabilities, and, therefore, have access to classified intelligence only indirectly through the regional chain via the CASFU or through the federal security manager at larger (Cat X) airports. In addition, most sensitive, but unclassified information that is disseminated is often seen as general and vague, and not highly valued by FAA regional and field personnel or by the airports and airlines. In the absence of national information, the airports and airlines claim they rely most heavily on CNN (Cable News Network) and, then, on local FBI and police information for threat information. The threat and vulnerability assessment process seemed to be little or poorly used, and neither FAA nor airport and airline personnel felt that they were especially valuable.

In the absence of a convincing, immediate threat, airport and airline security personnel seem to have increasingly transformed their concerns from the potential terrorist threat to that posed by compliance violations from ACS inspectors. FAA, in turn, seems to respond more to congressional or public criticism than to real or perceived changes in potential terrorist threat. Indeed, ACS set and has maintained a very high state of aviation security readiness since January 1996. Policy and enforcement variances seem to correlate more closely with public and political changes, than threat variations. Airport and airline security personnel, on the other hand, see violations as adversely impacting, or even endangering, their personal and professional careers much more immediately than the uncertain prospects of terrorist incidents.

- **Communications:** Communications among FAA levels and among the aviation security partners are also seen as a source of concern. The limited utility of the ASAC as a forum for information exchange and the problems associated with FAA field involvement in policy and intelligence matters are discussed above. In addition, there are different communication chains to federal security managers and other field personnel and, sometimes, different interpretations of guidance that frustrate both

FAA and airport and airline security personnel. The cumulative impact of dissatisfaction with participation in the formulation of regulations, inadequate supplemental guidance in plans and programs, unannounced security inspections, and untimely civil penalty enforcement serves to isolate the partners and thwart information exchange.

In summary, the status of the tripartite aviation security relationship is increasingly strained by an exceedingly lengthy regulatory processes, often imprecise regulations, aggressive compliance testing, and extended adjudicatory proceedings that are seen as more punitive than corrective, thus impeding cooperation. The FAA has a tough job maintaining motivation in the absence of adequate field understanding and acceptance of the threat of terrorism, but it is made more difficult by insufficient information exchange.

Security Practices

Variations among airports and airlines are often cited as reasons for the lack of specificity and crispness of FAA regulations and the policies and procedures that support them. Indeed, most airports argued against a standard security plan, such as that in place for air carriers, because of physical, technical, and structural differences. In connection with the draft FAR 107 revision, it has been suggested that the FAA propose a more standard approach to airport security plans rather than the 450 individual plans currently in existence. Irrespective of this potential major regulatory change, there appears to be a need to compile, evaluate, and disseminate aviation security practices that are efficient and effective in the variety of situations and circumstances the airports and airlines experience.

Initial inquiries at FAA headquarters and field locations, the airports, and airlines indicated that the variety of aviation security practices in effect is considerable, but that there is a lack of familiarity with the variations that might be possible. Airport security coordinators were not acquainted with alternatives practices even within the limits of the Washington DC metropolitan area. For example, Reagan National Airport charges employees a re-badging fee if an employee's badge is pulled because of failure to display a badge or failure to challenge an unbadged employee. BWI was searching for an employee penalty approach, but unaware of National's practice. Similarly, the Port Authority of New York and New Jersey and Atlanta airports have aggressive award programs for employees who challenge and report unbadged personnel in secure areas.

Airports have also tried a variety of access control techniques to record employee accesses, curtail piggybacking, and monitor unattended access doors. Atlanta, for example, has over 350 closed-circuit TV monitors on access doors. Most are not monitored on a fulltime basis, but these systems allow reasonably high-confidence tracking of employee security violations. Other airports report a high degree of success with turnstile-type access control devices, though their utility for access to certain baggage areas is probably limited. The industry uses a number of different devices that can record badged entries, departures, expirations, losses, and temporary or restricted access authority, but the industry's experience with specific devices is poorly recorded

and not widely shared. FAA staff often cited a reluctance to endorse specific techniques or vendors out of fear of charges of favoritism, as well as concern that their implicit approval of specific security techniques may conflict with their enforcement mission.

In addition, there is a wide range of industry experiences affecting screening activities. Differences in personnel training, pay, and turnover rates among airports, airlines, and screening companies have often been cited as factors affecting the effectiveness of screening activities. Industry security practices in terms of standards, experiences, practices, and assessments in these areas might be profitably shared to enhance aviation security.

FAA's aviation security clientele is widely scattered among 450 airports of differing configurations, capabilities, and competencies. While the one-size-fits-all approach to aviation security is almost certainly inappropriate, the dispersion of airports seems to be all the more reason why a clearinghouse of efficient and effective aviation security practices should be encouraged and advanced. ACS has manuals to guide federal security managers at major airports, but these are dated and not particularly helpful in advising security coordinators of evolving security technologies and/or procedures.

Addressing Public and Political Perceptions

Despite the strained relationship among the three aviation security partners, the United States aviation security program appears to have been remarkably successful in deterring terrorist or other interference. Hijackings, the original impetus behind the original air marshals program, have virtually disappeared as a threat, and the last hijacking attempt in the United States occurred in 1991. Aviation security's shift to concern with the introduction of explosives on commercial aircraft was dramatically heightened by the Pan Am 103 tragedy. There are at least some indications that shifted emphasis has helped deter and/or thwart terrorist attacks on US aviation. The number of attempts to introduce weapons aboard aircraft remains substantial, but most appear to be benign in intent. Increasingly, passenger and carry-on luggage screening appears to be effective in detecting violations, and this trend is likely to be considerably enhanced as new screening equipment is deployed and screening companies are certified. The aviation security posture in the United States remains brighter than that abroad, however, and foreign incidents against US civil aviation there remain a continuing source of concern.

Nonetheless, the public and political perception appears to be both unappreciative of the success of aviation security to date and unrealistic in its expectation for the future. Despite ACS regulations, the development, acquisition, and deployment of advanced technology equipment, and increased inspection and/or enforcement, there is a strong consensus that dedicated terrorists would be able to circumvent aviation security measures, board, plant a weapon aboard, or direct a weapon at, an aircraft, and precipitate a major aviation incident. The technical and procedural loopholes that make this possible are real, whether through breaching an airport's perimeter, introducing undetectable toxins or biological contaminants, or off-airport missile or electronic attacks on aircraft.

There does not seem to be a common appreciation of the prospects, problems, and limits of aviation security by the aviation security partners, the public, and the nation's political leadership. FAA has established aviation security as a key objective in its strategic plan and included it in its performance plan. Its performance measures, though unclassified, are sensitive and not subject to public review. Therefore, FAA's stated 2000 security goal, which is to prevent security incidents in the aviation sector, is difficult to observe and measure publicly and probably impossible to achieve. Zero tolerance of security risks may be politically attractive, but may generate totally unrealistic expectations. In addition, ACS' last annual assessment of aviation security, required by Congress, covers only up through 1997, and is not widely disseminated. (A new biennial version covering 1998 and 1999 is not yet finished.). ACS does produce a timely and useful assessment of incidents of civil aviation interference, but FBI and Department of State assessments of domestic and international terrorism are dated and not compelling.

The security relationship among FAA, airports, and airlines may only succeed with a shared appreciation of the realistic prospects and limits of aviation security. Congress' response to incidents or perceived threats is to call on the FAA to explain its regulations and the status of implementation and to press for stricter enforcement. FAA's response is often seen as a way of deflecting criticism, not necessarily advancing security. The airports and airlines seem genuinely concerned with FAA's vulnerability to the pressures of both the executive branch and Congress to respond to security concerns. The TWA 800 incident generated considerable pressure on the aviation security partners to undertake major technical programs and procedural changes, though their contributions to overall aviation security seem to be poorly understood. There is considerable concern about "flavor-of-the-day" enforcement, currently focused on access controls; repeated forays by external inspectors seem to be picking away at the fabric of the current security regime at the expense of the airports and airlines.

RECOMMENDED AREAS OF STUDY FOR PHASE II

1. The Panel believes that the FAA's regulatory process for aviation security can be substantially improved by increasing industry and regional participation, improving the feasibility of compliance through realistic cost-benefit considerations, decreasing the time required for issuance, and reducing the number of special orders associated with regulatory amendments. The role of the ASAC and other mechanisms for active industry participation and field involvement need to be assessed, and a more thorough analysis of the current timelines for regulatory actions, including actions beyond the immediate purview of ACS, is required. FAA's Civil Aviation Security acting administrator indicated that many proposals to improve the regulatory process have already been considered at length. Consequently, further review was seen as unlikely to appreciably advance this study's objectives. **The Panel clearly believes further improvements are attainable and proposes a review of the regulatory process focused on aviation security, leading to specific recommendations for regulatory changes and improved regulatory processes in this area. At a minimum, this review should look at ways to reduce the time associated with the regulatory**

process, to increase collaboration and industry participation through new or modified advisory bodies, and to improve the quality and use of cost-benefit considerations in designing security rules.

2. The Panel further believes that major modifications to aviation security inspection, compliance testing, and enforcement programs that would improve cooperation and coordination among the partners are desirable. The FAA's approaches to compliance in the areas of airport certification, air safety and flight standards, for example, emphasize greater reliance on FAA-approved and monitored self-inspection and self-disclosure so as to promote cooperation. Similarly, security inspection and testing activities could stress greater cooperation among the three aviation security partners, incorporate increased elements of airport and airline self-testing and reporting, test the effectiveness of greater reliance on individual accountability, and help generate a more timely, meaningful, and focused civil penalty process. **The Panel proposes further review to construct modified comprehensive assessment and compliance testing programs, possibly in the form of pilot modules for trial and testing. This review should include explicit consideration of FAA-approved and monitored self-testing activities by the airports and airlines and the impact of increasing individual accountability for security violations, and should consider streamlined alternatives to the current adjudication process.**
3. The Panel also believes successful cooperation among the aviation security partners will require development of a common interagency appreciation of security and threats and improved communications among the partners. Some of these may result from the detailed Phase II reviews directed at regulatory process improvements, inspection, compliance, and enforcement changes, as well as the security practices review cited below. **The Panel proposes to develop specific recommendations to improve communications among the security partners. Specific clearinghouse approaches and experiments that facilitate communications among the partners would be considered.**
4. There are several governmental organizational issues that also need attention, including where the responsibilities should lie for determining aviation security readiness levels, for establishing the balance between security consideration and passenger processing efficiencies, and for assessing the tradeoffs among technologies, resources, and priorities. These are not easy issues. In its response to a draft of this report, FAA indicated security readiness levels are already determined in coordination with the Intelligence Community and the National Security Council and subject to review by the Secretary of Transportation and the FAA Administrator. The Panel does not propose to conduct a comprehensive resource assessment, but rather an assessment of whether the FAA's organizational assignments and resource allocation and priority-setting processes appear adequate. **The Panel proposes Phase II address whether the FAA's organizational responsibilities for determining security readiness levels, balancing security and non-security**

considerations², allocating resources, and setting priorities are properly placed and whether other organizations should assume greater roles in these activities.

5. The Panel believes it will be useful to develop mechanisms to share efficient and effective practices for airport and airline security. The aviation security partners have no formal, structured means to share security approaches and report on the success or failure of specific security techniques. A common manual or, preferably, an electronic clearinghouse of security practices could serve as a guide for both federal security managers and field inspection units, facilitate updates as new techniques and technologies evolve, and be available, possibly through the Internet, to the industry's aviation security professionals. It could supplement, if not eventually replace, outdated FSM manuals. **During Phase II, the Panel proposes to develop a framework for a security practices manual or on-line clearinghouse, including examples of efficient and effective approaches, and a strategy for evaluating and disseminating aviation security practices and results.**

6. The Panel believes unmerited public concerns and unrealistic expectations by policy makers that absolute invulnerability can be achieved are among the most critical problems in aviation security. The aviation security partners need to speak with a coherent, coordinated, and consistent voice to the public and policy makers on aviation security matters. Periodic timely reports, agreed-upon by the aviation security partners, that address the nature and extent of the security threat, the status of US aviation security, the priorities associated with correcting deficiencies, and FAA's, airport, and airline performance will help. It will be necessary to protect sensitive information on specific aviation vulnerabilities in public reports, but policy and political agreement is also desperately needed. Unfortunately, there is no counterpart to the National Transportation Safety Board (NTSB) in aviation security to act as the definitive arbiter in security incidents and to temper the worst tendencies of some media and politicians. But it would be useful if both the Executive Branch and the Congress curb a natural tendency to overreact to suspected security incidents. **The Panel believes that further efforts to educate both the public and the political leadership about current aviation security realities are essential. During Phase II, the Panel proposes to:**
 - **Address measures that Congress and the Executive Branch might use to document the real progress by, and the realistic limits on, the aviation security partners**
 - **Develop an outline for, and major components of, collaborative reports as the first element of a joint educational strategy**
 - **Explore process and/or institutional alternatives, such as an NTSB for aviation security, that might help avert potential overreaction.**

² FAA indicated that "balancing security and non-security considerations is not in keeping with its statutory mandate of "maintaining and enhancing safety and security as the highest priorities in air commerce."

PANEL AND STAFF

PANEL

Alan L. Dean *Panel Chair*—Consultant. Former Vice President for Administration, U.S. Railway Association; Deputy Assistant Director, U.S. Office of Management and Budget; Assistant Secretary for Administration, U.S. Department of Transportation; Associate Administrator for Administration, Federal Aviation Agency.

David O. Cooke—Director of Administration and Management, U.S. Department of Defense. Former Deputy Assistant Secretary of Defense (Administration); Director, Organizational and Management Planning, U.S. Department of Defense; Captain, U.S. Navy.

Michael E. Levine—Adjunct Professor of Law, Harvard Law School. Former Executive Vice President, Marketing and International, Northwest Airlines; Dean, Endowed Chairs, Lecturer in Law, Yale University, School of Organization and Management; Henry R. Luce Professor of Law and Social Change in the Technological Society, California Institute of Technology; Professor, Associate Professor, and Assistant Professor of Law, University of Southern California; President and Chief Executive Officer, New York Air; Executive Vice President, Marketing, Continental Airlines. Former positions with U.S. Civil Aeronautics Board General Director, International and Domestic Aviation; Director, Bureau of Pricing and Domestic Aviation; Attorney (policy analysis).

Len Limmer*—Aergo Aviation Partners; Advisor, National Research Council's Panel on Assessment of Technologies Deployed to Improve Aviation Security. Former Deputy Executive Director of Airport Operations, Dallas/Fort Worth International Airport Board; Member and Chairman, Airports Council International's North American and World Standing Security Committees; Chief of Police of Mesquite, Texas.

Richard Monteilh—President, D.C. Chamber of Commerce. Former Director, Department of Housing and Community Development, Washington, D.C. Former Executive Director, Metropolitan Atlanta Olympics Games Authority; Chief Administrative Officer, City of Newark, New Jersey; Deputy Chief Administrative Officer and Deputy Commissioner of Finance, City of Atlanta; Deputy City Manager, City of Savannah; Staff Consultant, Governor's Office, State of Washington; Consultant, Booz Allen & Hamilton Management Consultants; Program Manager, International City Management Association.

Philip A. Odeen—Executive Vice President, Washington Operations, TRW, Inc. Former President and CEO, BDM International, Inc., Former Vice Chairman, Management Consulting Services, and Regional Managing Partner, Coopers & Lybrand, Washington, DC; Director of Program Analysis, National Security Council; Principal Deputy Assistant Secretary of Defense for System Analysis, U.S. Department of Defense.

* Not an Academy Fellow

Cindy Williams—Senior Fellow, Security Studies Program, Massachusetts Institute of Technology. Former Assistant Director, National Security Division, Congressional Budget Office. Former positions with MITRE Corporation: Director, C2 Integration Environment; Associate Technical Director, Continental Command, Control, and Communications Division; Department Head, Strategic Air Command Systems Department; Associate Department Head, Strategic Defense Initiative. Former positions with the U.S. Department of Defense: Director, Strategic Offensive Forces Division, Program Analysis and Evaluation, Office of the Secretary; Operations Analyst. Former positions with RAND Corporation: Mathematician, Strategic Forces Project; Project Leader, Force Operations Team, Automated Wargaming Center.

STAFF

J. William Gadsby, *Responsible Staff Officer*. Director of Management Studies, National Academy of Public Administration; project director on recent Academy studies of the management and operations of the Corporation for National Service and the Department of Housing and Urban Development. Former Senior Executive Service; Director, Government Business Operations Issues, Federal Management Issues and Intergovernmental Issues, General Accounting Office.

Arnold E. Donahue, *Project Director*. Consultant on defense, intelligence and information technology; project director on recent Academy studies on military sex crime investigations (1999), geographic information (1998), and the global positioning system (1995). Former Senior Executive Service; Chief, Intelligence and Command, Control, & Communications, U.S. Office of Management and Budget; Intelligence Officer, CIA.

Kenneth F. Ryder, *Senior Consultant*. Consultant on economic, financial, banking and housing issues. Former Senior Executive Service; Executive Director, Research and Analysis, Office of Thrift Supervision; Positions with the U.S. Office of Management and Budget, including Deputy Associate Director, Housing, Treasury and Finance Division and Deputy Associate Director, Special Studies Division, Economics and Government; Economist, the Rand Corporation.

Joseph P. Mitchell III, *Research Assistant*. Adjunct Professor, Center for Public Administration and Public Affairs, Virginia Polytechnic Institute and State University. Ph.D. (Public Administration and Public Affairs), Virginia Polytechnic Project Manager, Center for Transportation Research, Virginia Polytechnic.

Matthew A. Lewis, *Research Assistant*. Law student at Georgetown and majored in political science as an undergraduate at Yale University.

Martha S. Ditmeyer, *Project Assistant*. Staff, Management Studies Program, National Academy of Public Administration. Former staff member, Massachusetts Institute of Technology and the Communications Satellite Corporation, Washington, D.C. and Geneva, Switzerland.