

# THE CIP REPORT

APRIL 2004 / VOLUME 2, NUMBER 10

## Air Transportation

Aviation Security Post 9/11 . . . . .	2
FOIA Exemption . . . . .	3
Meet Reagan National's Federal Security Director . . . . .	5
Legal Insights . . . . .	6
Security Legislation Table . . . . .	7
Airports Council Int'l . . . . .	8
FAA's GAIN Program . . . . .	9
Airlines 101 . . . . .	10
NCR / CIVA Project . . . . .	13
CIPP Research on Transportation Security . . . . .	14

## CIP Project Staff

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Rod Nydam, *Associate Director, Private Sector Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: [cipp01@gmu.edu](mailto:cipp01@gmu.edu)  
703.993.4840  
If you would like to subscribe to *The CIP Report* please click [here](#).

No other industry has been more scrutinized than aviation since September 11, 2001. Since the advent of flight over one hundred years ago, safety has always been an issue. Security became a serious issue in the early 1970s with a rash of hijackings. Over the last thirty years, the industry implemented progressively sophisticated security techniques including passenger metal detectors, baggage x-rays, tighter airport and aircraft security, and beginning in the 1990s following the first World Trade Center bombing, passenger screening.

But the terrorist attacks on 9/11 and the subsequent passage of aviation security legislation turned the industry on its head and changed the system from one focused on efficiency to one subsumed by security issues.

This issue of *The CIP Report* focuses on the air transportation sector and on many of the security initiatives that have been launched over the last two

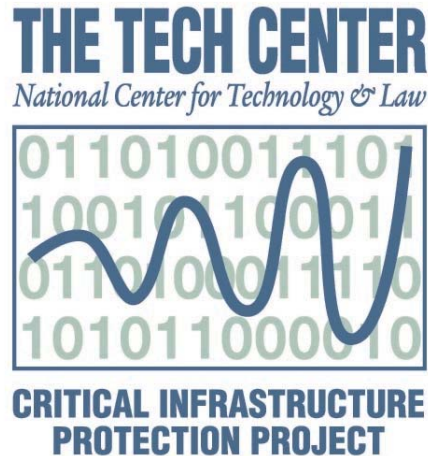
and a half years. The Aviation and Transportation Security Act of 2001 created the Transportation Security Administration, shifting responsibility for aviation security from the Federal Aviation

Administration to TSA. This issue provides information on many of TSA's security initiatives such as CAPPs II, advanced explosives detection systems, explosives trace detection machines, and the Federal Air

Marshal program.

The issue also includes information on various industry associations and legislation passed and pending, and introduces you to some industry officials closely involved in security issues.

Aviation is a critical infrastructure of particular interest to all of us. Even if our official duties are unrelated to aviation, most of us do fly at least occasionally. We hope that you find this issue of *The CIP Report* informative, whether for personal or professional reasons.



# AVIATION SECURITY IN A POST-9/11 WORLD

## The Transportation Security Administration's Aviation Security Regime

Since the Fall of 2001, great strides have been made in aviation security. The Transportation Security Administration (TSA) and the broader Department of Homeland Security (DHS) have spearheaded this effort. The goal that they have set before themselves is a civil aviation security system that provides both world-class security and world-class customer service.

TSA is putting into place a system that is dramatically different than any that we have known in the past. Historically, efficiency was valued above all, but since 9/11, that philosophy is no longer tenable.

Central to the new strategy at TSA is the concept of "rings of security," in which many layers, or rings of security, are in place at the same time. They overlap in many areas, and each of them directly contributes to overall security, but in the end none of

the rings are relied on exclusively.

TSA has invested enormous effort into researching the threats, vulnerabilities, and trends of the current security environment. Indeed, this is the first of the rings of security: domain awareness. The knowledge TSA has gained from this research and analysis has given TSA the confidence to set the agenda in aviation security, from allocating precious resources on one hand to taking preemptive action when necessary on the other.

Since 9/11, TSA, along with the Federal Aviation Administration (FAA), has been extremely busy. At local airports around the country, perimeter security has been vastly upgraded, with improvements coming in improved perimeter access roads, access control, electronic surveillance, intrusion detection, and security fencing. The system of personnel

hiring and training has been completely overhauled. More than one million air carrier and airport employees have undergone background checks. Screeners are now proficient in the use of advanced metal detectors and X-ray technology. Since February 2002, TSA has intercepted more than 1,600 firearms and over 58,000 box cutters. All the while, they have maintained a high degree of professionalism and diligence in all of their work.

It requires a monumental effort to ensure, every time you board a plane, that no one has been able to gain access to the aircraft carrying illegal items. Every piece of checked luggage is tested for explosives, and throughout the airport terminal, TSA-certified canine teams perform numerous missions every single day. Dogs aid with the screening of checked bags and unattended baggage, and they help to search vehicles that approach terminals during increased threat levels. They also play a lead role in responding to bomb threats.

The number of Federal Air Marshals (FAMs) has risen from a bare handful to the thousands. They are currently deployed both on high-risk domestic and international flights. And with the transfer of the FAM Service from TSA to the Bureau of Immigration and Customs Enforcement (ICE), DHS has the flexibility to augment this force by deploying ICE agents as a *(Continued, Page 3)*



**Deputy Secretary of the  
Department of Homeland Security  
Admiral James Loy**

Prior to being sworn in as Deputy Secretary on December 4, 2003 Admiral Loy served as the Administrator of the Transportation Security Administration. Admiral Loy retired from the Coast Guard as its Commandant on May 30, 2002. As

Commandant of the U.S. Coast Guard from May 1998 to May 2002, he focused his leadership on restoring readiness and shaping the future. Admiral Loy graduated from the U.S. Coast Guard Academy in 1964 and holds two master's degrees, one from Wesleyan University and one from the University of Rhode Island.

**Aviation Security** (Cont. from Page 2) surge force that will increase the number of federal agents on high-risk flights during periods of higher threat.

Commercial aircraft operating within the United States are now equipped with hardened cockpit doors. Furthermore, the Federal Flight Deck Officer program has the authority to train, equip, and deputize pilots who volunteer to defend the flight decks of passenger aircraft as the last line of defense. At the current application rate, TSA soon expects to have trained the vast majority volunteers who have met the initial background requirements.

Before 9/11, intelligence sharing in and around the Beltway was not where it should have been. These days, the pooling of intelligence resources is one of the most critical aspects in national defense strategy. TSA currently benefits from the resources of many agencies, both within the intelligence community and within law enforcement circles. Within DHS, TSA has the Information Analysis and Infrastructure Protection Directorate (IAIP), which has the responsibility for receiving and analyzing information that relate to threats to the homeland of all types. TSA's Office of Intelligence makes requests to various agencies based upon perceived threats, and then receives information in both raw and finished formats. In many cases, TSA now has the electronic connectivity it needs to many intelligence community databases, in order to

remain aware of the threats that other agencies are focusing on.

Even with all this connectivity, it has proved invaluable for TSA to have representatives actually posted on-site at other sites within the intelligence and law enforcement communities. This helps to ensure that all threats to transportation security can be passed to TSA as quickly and efficiently as possible. For example, TSA has two liaison officers assigned to the Terrorist Screening Center (TSC) adjudicating nominations for TSA watch lists. Beyond that, TSA also supplies detail personnel to assist operations at the TSC call center.

When TSA receives information from the intelligence community and law enforcement agencies, whether or not it specifically relates to transportation, it is always reviewed for potential impact on any U.S. transportation assets. The specific threat actors, their capabilities, their motivation, previous operations, and possible locations are all examined in detail. Next, TSA coordinates with all DHS Directorates to review security measures that are already in place, as well as the status of targeted transportation assets. A determination is then made regarding the viability of a threat and the chances that a terrorist operation might be successful. The traditional formulas regarding the original source of the information are also applied when assessing the risk. How credible is the source, and how reliable the new information?

## FOIA EXEMPTION FOR AVIATION SECURITY

Shortly after 9/11, President Bush signed the Aviation and Transportation Security Act (PL: 107-71) into law and expanded Freedom of Information Act exemptions to all transportation issues. Prior to the bill's passage, only aviation-related information could be protected from disclosure to the general public. Lawmakers were concerned after the attacks that vulnerability data about the country's transportation systems could be exploited by terrorists.

Congress assigned the Transportation Security Administration the task of drafting regulations to implement the law's FOIA provisions. TSA classified many new categories of information as "sensitive security information" that could be protected from disclosure, including the following:

- Selection criteria used in any security screening process, including criteria for persons, baggage, or cargo;
- Securities contingency plans;
- Any information that TSA determines may reveal a systemic vulnerability in the aviation system;
- Information concerning threats against transportation; and
- Information in a vulnerability assessment that has been authorized, approved, or funded by the Department of Transportation.

Only after all of this is done is TSA able to complete a comprehensive threat and vulnerability assessment.

One of the most visible ways in which TSA (Continued, Page 4)



**Aviation Security** (Cont. from Page 3) amplifies potential threats to the transportation industry is via dissemination of watch lists, which enumerate the individuals known or believed to be a threat to civil aviation. TSA



**John Luke III, C.M.**  
Airport Manager  
Montgomery County  
Revenue Authority

“Providing security at a busy general aviation airport closer than 20 miles from the White House naturally poses a challenge. In the absence of a federal mandated security program, you rely not only on your physical surroundings (security fence, code controlled access gates, deterrent signage, etc.,) but also on your locally based pilot population to be the eyes and ears of your informal security force. These people know and can tell who should be on the airfield at a given time and are not bashful to challenge anyone who looks or acts suspicious.”

also writes several daily products, at both the classified and unclassified levels. Each of them provides information that is of security interest to DHS and to other agencies both inside the Beltway and around the nation.

In the event that the level of threat is high enough to justify an official warning to industry, TSA has numerous options at its disposal. The top decision makers in government can be alerted immediately, so that they are able to quickly leverage any other national-level resources that need to be brought to bear. TSA operates a 24/7 Transportation Security Coordination Center (TSCC) that coordinates all security-related operations vis-à-vis all modes of transportation. If the incident calls for detailed warnings to be written, TSA puts out products entitled Information Circulars, which may provide specific guidance on what security measures for industry stakeholders should implement.

Throughout the United States, one of the most important roles has become that of the Federal Security Director (FSD), of which there are now 158. The FSD is responsible for coordinating all TSA security activities at airports, to include the planning, execution, and management of operations. All of the FSDs arrive at TSA from distinguished careers. Their ranks include Flag Officers from the military, special agents from the FBI, Secret Service, and Drug Enforcement Administration as well as top industry executives.

In order to properly secure the

transportation sector from terrorist attack, it is vital that the private sector play a robust role in all aspects of the effort. This partnership between the government and industry cannot be overstated. In fact, industry stakeholders must now be held accountable for their own, delineated contributions to transportation security. This includes air carriers, airports, and transportation operators. This is an evolving relationship, and currently TSA has a progressive enforcement policy that stresses immediate corrective action ahead of the imposition of civil penalties.

In terms of security technology, TSA's goal is to stay at least one step ahead of those wanting to do harm. TSA has invested enormous effort into building research and development that is robust, which works closely with the DHS Science and Technology Directorate to develop and deploy security technologies that will make the nation's transportation security more effective, more efficient, and less expensive to maintain. TSA is currently testing explosives trace detection portals that passively analyze the air for explosive material as passengers walk through them. Its scientists are also developing a document scanner that can detect traces of explosives on any documents that a passenger may have been holding.

TSA is continuously evaluating its own security procedures and vulnerabilities. It employs robust, covert "red teaming" that challenges its employees to detect many (Continued, Page 15)

## 'Every Day is Opening Night' for Reagan National Airport Security

Pat Hynes began his federal law enforcement career in 1970 with the FBI, and later joined the Bureau of Alcohol, Tobacco, Firearms and Explosives as a special agent where he rose to the position of deputy director. He now works for the Transportation Security Administration serving as the Federal Security Director (FSD) for Reagan National Airport. The position of FSD was created by the Aviation and Transportation Security Act signed by President Bush on November 19, 2001.

FSDs are directly responsible for a full range of airport security enforcement and oversight at all of the nation's airports, with duties including:

- The efficient implementation, performance and enhancement of security and screening standards for TSA employees;
- Airport security risk assessments;
- Supervision of federal law enforcement activity within the purview of the TSA; and
- Organizing and implementing the Federal Security Crisis Management Response Plan for each airport.



**Patrick D. Hynes**  
Federal Security Director  
Ronald Reagan Washington  
National Airport

When asked how he manages so many critical responsibilities, Mr. Hynes explained his metaphor of a three-legged stool. One leg is the Airport Manager and Chief of Police, who represent the Airport Authority; one leg is the air carriers; and TSA is the third leg. "Nothing is done at this airport without the collaboration of all three. This is a partnership." In fact, Mr. Hynes begins each day in a meeting with Chris Browne, the Airport Manager, who he credits with playing an integral role in TSA's mission and success at Reagan National.

One of the biggest challenges for Federal Security Directors is integrating world-class security with world-class customer service. "We are making a commitment to the flying public that when they step onto an airplane it is safe, because we have screened every person, every piece of baggage and all of the cargo that is on board. But we also want to provide top of the line customer service, which isn't always easy with so many security constraints."

Mr. Hynes' tool belt for tackling this job includes professionally trained screeners, state of the art explosives detection and trace equipment, a canine force trained in explosives detection, and a covert training group. Each morning he receives a readiness report which enables him to ensure that the airport's security mission has 100% of the required resources. Hynes is also in constant communication with the intelligence community and the FBI, particularly because of the high-profile nature of the airport.

"This is the Nation's Airport. With so many heads of state, politicians, top industry representatives, other VIP's, and millions of tourists passing through our gates, we must always be at our best. My motto is 'Every day is opening night.' We must never forget why the Department of Homeland Security was formed, and our work must never become mundane or routine. We have to get it right every single time."

by Emily Frye

## CAPPS II and the Fourth Amendment: Does It Fly?

by Guest Columnist  
Deborah v. Rochow-Leuschner

The worst international terrorist attack ever-involving four separate but coordinated aircraft hijackings-rocked the United States on September 11, 2001 killing more than 3,000 random victims. Although hijackings have plagued the airline industry since its inception, this new breed of mass-murder suicide hijackers has brought the airlines to the brink of ruin.

As a result of inadequacies in airline security, the government stepped in and federalized the entire airport screening industry. The crown jewel of the new Transportation Security Administration (TSA) is a powerful networked database system that runs a background check on every single passenger in the time it takes to get a boarding card. The purpose of the Computer Assisted Passenger Prescreening System II (CAPPS II) is to analyze various factors in each traveler's background, and then to predict whether a person poses a potential threat to the flight.

Travelers will receive a red, yellow or green score. The majority of travelers will get a green light, and will pass through standard security procedures, making the process more efficient for all. In the random system previously used, grandmothers were as like-

ly to be searched as young Arabic men. If something in the traveler's background triggers a yellow score, that person may be questioned, and both carry on and checked baggage will be searched. Law enforcement will be called in to question travelers with a red or "no fly" indicator. It is unclear which 5th amendment protections will apply in this case.

The program is controversial because of the myriad individual factors that are analyzed in determining a person's threat level. Further, most elements of the profile are classified to prevent terrorists from undermining the system. At a minimum, the CAPPS II background check will include an FBI check, credit check, analysis of financial and transactional records, and travel patterns. The complex algorithms will look for evidence that a traveler is "rooted in the community."

Although the TSA believes that this program will be highly effective in preventing potential terrorists from ever boarding an aircraft, the program's critics believe CAPPS II is an abject invasion of privacy. Trying to predict a person's behavior is like searching for "thought crimes." Never before has so much information from so many sources been collected in a single place. The "digital dossiers" may fall into the

wrong hands. "Function creep" is inevitable as the IRS, law enforcement, and various other agencies seek access to the data. Furthermore, people may be arrested at the airport or denied the right to travel because of infractions that have nothing to do with security of the flight. Racial, ethnic, and even gender discrimination will rear its ugly head as people are scrutinized based on immutable characteristics. Further, the error rate may be unacceptable. If just one percent of the population scores a false positive, more than 6 million unjustified inquiries are performed per year.

The Fourth Amendment protects Americans' privacy from invasive "search and seizures" whether physical or virtual. The landmark case *Katz v. United States*, 389 U.S. 347 (1967) pronounced that privacy protects people not places, and if a person has an actual and reasonable expectation of privacy, the government may not violate this interest without probable cause and a warrant. Most travelers are unaware of the background checks being surreptitiously performed, and would reasonably expect that their personal information is private. So how will CAPPS II comply with the Fourth Amendment?

The paper (*Continued, Page 15*)

## Aviation Security Bills

<i>Bill</i>	<i>Status</i>	<i>Description</i>
To provide for the arming of cargo pilots (HR 3262)	House Committee on Transportation and Infrastructure	Amends Federal transportation law to expand the Federal flight deck officer program (providing for the arming of pilots of passenger aircraft) to include pilots of cargo aircraft.
Aviation and Transportation Security Act (S.1447)	Became Public Law 107-71	A bill to improve aviation security that establishes a Deputy Secretary for Transportation Security who shall be responsible for: (1) security for all modes of transportation, including aviation-related security; and (2) domestic transportation during a national emergency; and directs the FAA to require employment investigations (including criminal history record checks) for all existing employees who have unescorted access to an aircraft or to secure areas of a U.S. airport.
Air Transportation Safety and System Stabilization Act (HR.2926)	Became Public Law 107-42	Directs the President to take certain actions to compensate air carriers for losses they incurred as a result of the terrorist attacks on the United States on September 11, 2001. Also, Dept. of Transportation to provide insurance and reinsurance against loss or damage arising out of any risk from the operation of an American aircraft or foreign-flag aircraft while in the U.S.
Securing Existing Aviation Loopholes Act (HR 3262)	House Committee on Transportation and Infrastructure	Amends the Homeland Security Act of 2002 to improve aviation security by: (1) requiring all cargo carried on passenger aircraft to be screened or inspected; (2) requiring all foreign air carriers departing from or arriving in the United States to have an air marshal on board; (3) improving aircraft communications systems; (4) improving preflight inspections of passenger aircraft for dangerous objects; and (5) improving airport access security.
Commercial Aviation MANPADS Defense Act of 2004 (HR 4056)	House Committee on International Relations	Expedites installation of equipment on commercial aircraft that could protect plans from shoulder-fired ground-to-air missiles.
To provide air marshal training to law enforcement personnel of foreign countries (HR 3959)	House Committee on Transportation and Infrastructure	Amends Federal law to authorize the Secretary of Homeland Security, through the Under Secretary for Border and Transportation Security, to provide air marshal training to foreign law enforcement personnel. Directs the Under Secretary to establish related fees.
Aviation Investment and Revitalization Act (HR.2115)	Became Public Law 108-176	Directs the Department of Homeland Security to study and report on the effectiveness of the aviation security system. Authorizes the establishment of an Aviation Security Capital Fund to provide financial assistance to airport sponsors to defray capital investment in transportation security at airport facilities. Requires the DHS to issue final regulations ensuring the security of foreign and domestic repair stations.
To permit certain local law enforcement officers to carry firearms on aircraft (S 2060)	Senate Committee on Commerce, Science, and Transportation	Directs the Under Secretary of Transportation for Security to prescribe regulations that permit qualified local law enforcement officers to carry accessible weapons while onboard an aircraft to the same extent and subject to the same limits as Federal law enforcement officers are permitted to do so.





## Airports Council International-North America (ACI-NA)

First established as the Airport Operators Council in 1947, the

Airports Council International-North America (ACI-NA) is the "Voice of Airports" representing local, regional and state governing bodies that own and operate commercial airports throughout the United States and Canada.

ACI-NA is the largest of six worldwide regions of Airports Council International (ACI), based in Geneva, Switzerland. Europe, Asia, Pacific, Africa and Latin America/Caribbean are ACI's other regions.

ACI-NA offers the pre-eminent North American airport forum for the exchange of ideas and information. Its staff is headquartered in Washington, DC and Ottawa, Canada, providing ACI-NA with direct access to the federal government, industry partners and related aviation associations.

As a member association, ACI-NA helps its members develop common positions and communicate them among the government, the press and the general public. ACI-NA is recognized

"Airport owners and operators have always recognized their overall responsibility for the safety and security of those who work and use their facilities. How security is accomplished at each airport is unique since all airports are different in design, physical infrastructure, as well as in their relationships with airlines and other constituencies. The aftermath of September 11th demonstrated the importance of aviation to both the local and global economies. Aviation is part of our critical infrastructure and it is essential that we work with the different federal agencies to develop smart security policies and procedures that enhance the overall security of our airports. Issues on the forefront for airports include perimeter security, passenger and baggage screening, cargo security, and maintaining a high level of customer service while ensuring the safety and security of all passengers."



**Ian Redhead**  
ACI-NA  
Vice President of Airport  
Facilities and Services

as the authoritative voice of airports, and represents airports that carry 98% of all passenger traffic - and almost all cargo traffic - throughout North America. Over 380 aviation related businesses are also Associate members of ACI-NA. The mission of ACI-NA states that ACI-NA shall identify, develop and advance common policies and programs for the enhancement and promotion of airports and their managements that are effective, effi-

cient and responsive to consumer and community needs.

ACI-NA's Public Safety and Security Committee provides a forum for airport security professionals to discuss sensitive security policies, programs and procedures and their implementation system wide. Like other committees of ACI-NA the PSS Committee strikes a balance between policy development and member education and information exchange. ❖



# Global Aviation Information Network

## Sharing Information to Make the Skies Safer

The Global Aviation Information Network is an industry-led international coalition of airlines, manufacturers, employee groups, governments and other aviation organizations formed to promote and facilitate the voluntary collection and sharing of safety information by and among users in the international aviation community to improve aviation safety.

The GAIN concept was proposed in May 1996 as a way to significantly improve aviation safety through the enhanced use of safety information. One of the prerequisites to the collection and sharing of safety information is the culture of the organization itself. Thus, GAIN is promoting the "just culture" concept, which describes an atmosphere of trust in which people are encouraged, even rewarded, for providing essential safety-related information - but in which they are also clear about where the line must be drawn between acceptable and unacceptable behavior. The policy of just culture is designed to encourage compliance with the appropriate regulations and procedures, foster safe operating practices, and promote the development of internal evaluation programs.

Over 1,000 aviation safety professionals from 54 countries have participated in the GAIN program since its inception in 1996. Organizations participating in GAIN include airlines, airframe manufacturers, avionics and safety software developers, employee

groups (pilots, mechanics, air traffic controllers, and flight attendants), civil aviation authorities, accident investigation boards, air traffic service providers, aviation trade associations, military aviation, and university groups involved in aviation safety.

"Most of the information sharing taking place is through informal networks, but we are in the process of making GAIN a systematic worldwide program," explains Christopher Hart, Assistant Administrator for System Safety at the Federal Aviation Administration. Two main areas of focus include legal, regulatory, and cultural issues that may deter information sharing, as well as development of analytical tools that can handle massive amounts

of safety-related information. Significant strides have been made in both of these areas.

According to Hart, one of the biggest challenges is bringing all of the various players together to create a system approach. "We can no longer look at components such as manufacturing or air traffic control in a vacuum. The safety issues of tomorrow are system issues that involve every link in the chain."

Four GAIN Working Groups accomplish the work of GAIN by studying issues, conducting or facilitating surveys and other research, compiling knowledge from group members and peers in other safety organizations, and documenting (*Continued, Page 13*)

### Christopher A. Hart Assistant Administrator for System Safety Federal Aviation Administration

Christopher A. Hart is a graduate of Harvard Law School, and he earned bachelor's and master's degrees in aerospace and mechanical science at Princeton University. He holds a commercial pilot's license with multi-engine and instrument ratings as well.



He served as a member of the National Transportation Safety Board (1990-93). While working at the Safety Board, he had specialized interests in human factors and the impact of automation on transportation systems.

Mr. Hart is a member of the Aircraft Owners and Pilots Association and the Lawyer Pilots Bar Association, and he has been listed in "Who's Who in Aviation." He has a connection in aviation history – in 1926, Hart's great uncle, James Herman Banning, became the first African-American to earn a U.S. pilot's license.

# AIRLINES 101

A refresher on the aviation industry, excerpted from *The Airline Handbook* by the Air Transport Association

## The Airline Deregulation Act

Today's airline industry is radically different from what it was prior to 1978. At that time, the industry resembled a public utility, with a government agency, the Civil Aeronautics Board (CAB), determining the routes each airline flew and overseeing the prices they charged. Today, it is a market-driven industry, with customer demand determining the levels of service and price.

The turning point was the Airline Deregulation Act, approved by Congress on October 24, 1978 and signed into law four days later by President Jimmy Carter. Pressure for airline deregulation had been building for many years, particularly among economists who pointed out, in numerous studies, that unregulated intrastate airfares were substantially lower than fares for interstate flights of comparable distances.

## What Remains Regulated

Among the CAB functions shifted to other parts of the government were the responsibility for awarding landing rights and other privileges in foreign countries to U.S. carriers. International air services are usually governed by air-transport service agreements, referred to as bilaterals, between two nations. These agreements specify such things as the cities each

nations' airlines may serve, the number of flights they may operate, and how much regulatory authority the governments will exercise over fares. Bilateral negotiations involving the United States are led by the State Department, with active DOT policy input and participation.

## Effects of Deregulation

A major development that followed deregulation was the widespread development of hub-and-spoke networks, which existed on a more limited basis prior to 1978. Hubs are strategically located airports used as transfer points for passengers and cargo traveling from one community to another. They are also collection points for passengers and cargo traveling to and from the immediate region to other parts of the country or points overseas. Airlines schedule banks of flights into and out of their hubs several times a day. Each bank includes dozens of planes arriving within minutes of each other. Once on the ground, the arriving passengers and cargo from those flights are transferred conveniently to other planes, that will take them to their final destinations.

## Types of Airline Certification

U.S. scheduled airlines are classified by the government on the basis of the amount of revenue generated from operations.

These classifications are major, national and regional. All airlines hold two certificates from the federal government: a fitness certificate and an operating certificate. The Department of Transportation (DOT) issues fitness certificates - called certificates of public convenience and necessity - under its statutory authority. Basically, the certificate establishes that the carrier has the financing and the management in place to provide scheduled service. The certificate typically authorizes both passenger and cargo service. Operating certificates, on the other hand, are issued by the Federal Aviation Administration (FAA) under Part 121 of the Federal Aviation Regulations (FARs), which spell out numerous requirements for operating aircraft with 10 or more seats. The requirements cover such things as the training of flight crews and aircraft maintenance programs. All majors, nationals and regionals operate with a Part 121 certificate.

Major airlines generate operating revenues of more than \$1 billion annually. Previously called trunk carriers, they generally provide nationwide, and in some cases, worldwide service. There were 12 major U.S. passenger airlines in 2000: Alaska, America West, American, American Eagle, American Trans Air, Continental, Delta, Northwest, Southwest, (Continued, Page 11)

**Airlines 101** (Cont. from Page 10) Trans World, United and US Airways. In addition, three all-cargo airlines were classified as majors: DHL Airways, FedEx and United Parcel Service.

### Chief Characteristics of the Airline Business

Because of all of the equipment and facilities involved in air transportation, it is easy to lose sight of the fact that this is, fundamentally, a service industry. Airlines perform a service for their customers - transporting them and their belongings (or their products, in the case of cargo customers) from one point to another for an agreed price. In that sense, the airline business is similar to other service businesses like banks, insurance companies or even barbershops. There is no physical product given in return for the money paid by the customer, nor inventory created and stored for sale at some later date.

Unlike many service businesses, airlines need more than storefronts and telephones to get started. They need an enormous range of expensive equipment and facilities, from airplanes to flight simulators to maintenance hangars. As a result, the airline industry is a capital-intensive business, requiring large sums of money to operate effectively. Most equipment is financed through loans or the issuance of stock. Increasingly, airlines are also leasing equipment, including equipment they owned previously but sold to someone else and

leased back. Whatever arrangements an airline chooses to pursue, its capital needs require consistent profitability.

Because airlines own large fleets of expensive aircraft which depreciate in value over time, they typically generate a substantial positive cash flow (profits plus depreciation). Most airlines use their cash flow to repay debt or acquire new aircraft. When profits and cash flow decline, an airline's ability to repay debt and acquire new aircraft is jeopardized.

Airlines also are labor intensive. Each major airline employs a virtual army of pilots, flight attendants, mechanics, baggage handlers, reservation agents, gate agents, security personnel, cooks, cleaners, managers, accountants, lawyers, etc. Computers have enabled airlines to automate many tasks, but there is no changing the fact that they are a service business, where customers require personal attention. More than one-third of the revenue generated each day by the airlines goes to pay its workforce. Labor costs per employee are among the highest of any industry. In part because of its long history as a regulated industry, the airline industry is highly unionized.

The bottom line result of all of this is thin profit margins, even in the best of times. Airlines, through the years, have earned a net profit between one and two percent, compared to an average of above five percent for U.S.

industry as a whole.

The airline business historically has been very seasonal. The summer months were extremely busy, as many people took vacations at that time of the year. Winter, on the other hand, was slower, with the exception of the holidays. The result of such peaks and valleys in travel patterns was that airline revenues also rose and fell significantly through the course of the year. This pattern continues today, although it is less pronounced than in the past. The growth in the demand for air transportation since deregulation has substantially lessened the valleys.

### Airline Revenue - Where the Money Comes From

About 75 percent of the U.S. airline industry's revenue comes from passengers; about 15 percent from cargo shippers, the largest of which is the U.S. Postal Service. The remaining 10 percent comes from other transport-related services. For the all-cargo carriers, of course, cargo is the sole source of transportation revenue. For the major passenger airlines which also carry cargo in the bellies of their planes, less than 10 percent of revenue comes from cargo (in many cases far less).

### Airline Costs - Where the Money Goes

According to reports filed with the Department of Transportation in 1999, airline costs were as follows: (Continued, Page 12)

**Airlines 101** (Cont. from Page 11)

- Flying Operations - essentially any cost associated with the operation of aircraft, such as fuel and pilot salaries - 27%;
- Maintenance - both parts and labor - 13%;
- Aircraft and Traffic Service - basically the cost of handling passengers, cargo and aircraft on the ground and including such things as the salaries of baggage handlers, dispatchers and airline gate agents - 16%;
- Promotion/Sales - including advertising, reservations and travel agent commissions - 13 %;
- Passenger Service - mostly inflight service and including such things as food and flight attendant salaries - 9%;
- Transport Related - delivery trucks and inflight sales - 10 %;

- Administrative - 6%;
- Depreciation/Amortization - equipment and plants - 6%.

Labor costs are common to nearly all of those categories. When looked at as a whole, labor accounts for 35 percent of the airlines' operating expenses and 75 percent of controllable costs. Fuel is the airlines' second largest cost (about 10 to 12 percent of total expenses), and travel-agent commissions is third (about 6 percent). Commission costs, as a percent of total costs, have recently been declining, as more sales are now made directly to the customer through electronic commerce. Another rapidly rising cost has been airport landing fees and terminal rents. ❖

*Founded by a group of 14 airlines meeting in Chicago in 1936, the Air Transport Association was the first, and today remains, the only trade organization for the principal U.S. airlines. In that capacity it has played a major role in all the major government decisions regarding aviation since its founding, including the creation of the Civil Aeronautics Board, the creation of the air traffic control system, and airline deregulation. The purpose of the ATA is to support and assist its members by promoting the air transport industry and the safety, cost effectiveness, and technological advancement of its operations; advocating common industry positions before state and local governments; conducting designated industry-wide programs; and assuring governmental and public understanding of all aspects of air transport.*

<b>Aviation Organizations and Website Links</b>	
American Association of Airport Executives Security Central	<a href="http://www.airportnet.org/security/">http://www.airportnet.org/security/</a>
Airports Council International - North America	<a href="http://www.aci-na.org">http://www.aci-na.org</a>
Airline Pilots Association International	<a href="http://www.alpa.org">http://www.alpa.org</a>
Air Transport Association	<a href="http://www.air-transport.org">http://www.air-transport.org</a>
The International Air Cargo Association	<a href="http://www.tiaca.org/">http://www.tiaca.org/</a>
House Subcommittee on Aviation	<a href="http://www.house.gov/transportation/">http://www.house.gov/transportation/</a>
Senate Subcommittee on Aviation	<a href="http://commerce.senate.gov/subcommittees/aviation.cfm">http://commerce.senate.gov/subcommittees/aviation.cfm</a>



## Local Universities Launch New Homeland Security Initiative

George Mason University (GMU), in cooperation with universities in Virginia, Maryland, and Washington DC, is leading a new homeland security initiative. The program, termed the Critical Infrastructure Vulnerability Assessment (CIVA) Project, aims to enhance safety and security in the 12 jurisdictions that comprise the National Capitol Region (NCR) by improving government and industry methods of identifying infrastructure vulnerabilities.

The NCR-CIVA Project is part of a broader Federal effort to protect the nation's urban areas. In 2002, Congress worked with the Administration to create the Urban Area Security Initiative (UASI), which provides funding for local safety officials and first responders to secure infrastructure and prepare for acts of terrorism. George Mason University, under a grant from UASI, founded the NCR-CIVA and partnered with James Madison University, the University of Virginia, Virginia Polytechnic Institute and State University, the University of Maryland, and Howard University.

The Project began work in late 2003 and was officially launched in March of 2004. In the beginning, the Project analyzed the effects of Hurricane Isabel on regional infrastructures and produced a detailed assessment of the interdependencies revealed by the storm. With the valuable experience gained from this effort, NCR-CIVA member universities began a series of activities focused on the DC area to improve the vulnerability assessment process. Currently, George Mason University is collecting and reviewing existing vulnerability assessment procedures, processes, and tools employed in the following infrastructure sectors: banking and finance, emergency services, energy, health services, postal and shipping, telecommunications, transportation, and water. Going forward, GMU and partner universities plan to collect information about private sector vulnerability assessments through discussions with infrastructure owners and operators.

After gathering and evaluating

components of these vulnerability assessments, NCR-CIVA universities will develop a best practice process for conducting them.

This will help ensure processes are coordinated and appropriately integrated so that security activities are effective, consistent, and cost-effective. While these best practice recommendations will support individual sector needs, they will also provide standard elements that allow for cross-sector comparisons for use in local, state, and regional critical infrastructure protection efforts. GMU also plans to provide policy and business practice recommendations for implementation of the NCR-CIVA Project findings.

The NCR-CIVA Project's vision is to develop an open standard for conducting vulnerability assessments. This open standard can evolve over time and incorporate new best practices as they are identified. Ultimately, the Project seeks to raise the level of security in the National Capital Region by ensuring that critical infrastructure sectors address the most important security concerns. ❖

**GAIN** (Cont. from Page 9) this information in GAIN reports. Groups meet several times each year, in person and by teleconference. Participation on Working Groups is open to all interested parties.

Many other industries, including other transportation modes, health care, national security, chemical manufacturing, nuclear

power, public utilities, and information infrastructure protection are similarly trying to develop programs to use information proactively to improve safety. GAIN is coordinating with them in order to make better use of scarce resources by avoiding duplication of efforts. "The tools and processes of using good information to figure out what almost went wrong, what factors con-

tributed to the problem, and what factors prevented an incident or accident are applicable to many other sectors in the areas of safety, critical infrastructure protection, and national security," said Hart.

GAIN's Seventh World Congress will be held September 28-30, 2004 in Montreal, Canada. More information can be found at [www.gainweb.org](http://www.gainweb.org). ❖

## Transportation Infrastructure Security: Innovative Technology for Vehicle, Operator and Cargo Identification

Michael S. Bronzini, Dewberry Chair Professor  
School of Information Technology and Engineering

The data required to protect critical infrastructure extends to information about vehicular traffic in transportation systems. Traditional traffic sensing and surveillance systems focus on macroscopic stream measures, such as traffic volume, speed and density, and vehicle classification. This CIP research project considers the threats to transportation infrastructure security, and focuses on the potential application of both traditional and innovative vehicle detection technologies for vehicle, operator, and cargo identification. The ultimate goal is to help create an infrastructure system with the ability to identify vehicles, operators, cargos and contents.

As a key phase of this project a two-day Faculty Workshop will be organized and held during late July or early August of 2004. The objectives of the workshop are to:

- Evaluate and critique current and near-term vehicle detection technologies;
- Evaluate and critique current and near-term vehicle identification system designs;
- Propose technologies to aid in vehicle detection and identification;
- Propose vehicle detection and identification systems designs;
- Propose demonstration of the use of an innovative technology;
- Decide on a research and

demonstration plan.

To support the workshop a technology scan working paper is under development.

The expected workshop outcomes include:

- A basic understanding of the benefits and limitations of current vehicle detection and identification capabilities for addressing CIP data needs;
- An outline of future research, engineering, and applications development;
- An interim consensus of which technologies (sensors and methods) hold the greatest promise for enhancing CIP applications involving vehicle,

operator, and cargo identification;

- A working agenda and technical plan for applications of vehicle detection and identification technologies to transportation infrastructure security.

Anyone interested in participating in the workshop should contact Dr. Bronzini at [mbronzin@gmu.edu](mailto:mbronzin@gmu.edu).



**ROD NYDAM**

Associate Director,  
Private Sector Programs  
Critical Infrastructure  
Protection Project  
George Mason  
School of Law

Rod Nydam recently joined the CIP Project team at George Mason Law School where he will be guiding private sector initiatives related to critical infrastructure protection. Prior to joining the CIP Project, Rod was corporate attorney and a partner in two large international law firms. Rod has been involved in critical infrastructure protection issues since early 2000 and has served on task forces related to both cyber and physical security issues. He has assisted in drafting and editing white papers related to the legal business issues surrounding private-public partnerships focusing on infrastructure protection and has also given speeches and presentations to legal, business and accounting groups on the importance of protecting corporate infrastructures.

Rod has a bachelor's degree in Economics from Cornell University and a JD from Cornell Law School with a focus in Economic and Business Regulation.

**Legal Insights** (Cont. from Page 6) "CAPPS II and the Fourth Amendment: Does It Fly?" appears in full in the March 2004 Southern Methodist University School of Law *Journal of Air, Law, and Commerce*. The author, an attorney and airline employee examines several exceptions to Fourth Amendment protections that have been carved out in recent years and how they might apply to virtual data searches. Some of these exceptions such as the administrative search doc-

trine have been used to permit the magnetometer screening in use in airports since the 1960s. Other possible justifications include the consent and implied consent doctrines, the stop and frisk exception, and the national security exception. The paper compares justifications for other invasive methods in the name of security sobriety checkpoints, drug testing, and border patrol stops.

The bottom line is the inevitable tradeoff between security and

privacy. Judges who like the protections offered by CAPPS II will find rationalizations in the Fourth Amendment for upholding it, and those who dislike the surveillance aspects will also find grounds in the Fourth Amendment for banning it. Travelers will also have diverse viewpoints. Plenty of people will welcome the added security, believing they have "nothing to hide." Others will see this as a slippery slope to totalitarianism. Time will tell. ❖

**Aviation Security** (Cont. from Page 4) employees to detect many different types of threats, at checkpoints around the country. They use stealthy, realistic scenarios, and currently operate at several times the frequency of previous iterations at the FAA.

TSA has taken great steps toward implementing another vital weapon to combat terrorists, known as the second-generation Computer Assisted Passenger Prescreening System (CAPPS II), which will greatly enhance TSA's ability to protect the commercial airlines while still allowing for the quick processing of passengers. CAPPS II will have the capability to authenticate the identity of passengers while performing an on-the-spot risk assessment to determine if someone is either a

terrorist threat or is the subject of an outstanding warrant for violent criminal behavior.

CAPPS II performs this important mission in two phases. It first attempts to verify the identity of each passenger by matching the limited information available, such as name, date of birth, or address, with commercially available databases. Next, CAPPS II performs a risk assessment, which is based upon a list of names that include known or suspected terrorists and those who are subject to an outstanding warrant for violent criminal behavior. Based on the traveler's "risk score", an encoded message will be printed on the boarding pass that will indicate the passenger's appropriate level of risk: green (no risk), yellow

(unknown or elevated risk), or red (high risk).

CAPPS II is a threat-based system that will be under the direct control of the Federal government. It will be a major improvement over the current CAPPS system, in which all threat-related information is disparate and under the control of airlines themselves. Throughout the testing and implementation of CAPPS II, DHS will be scrupulously mindful of the rights and freedoms that define our Nation and distinguish American society from those of the terrorists who seek to do us harm. ❖

*The information for this piece was extracted from Admiral James Loy's testimony to the National Commission on Terrorist Attacks Upon the United States, January 27, 2004.*

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Project. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for The CIP Report, please click on this link: <http://listserv.gmu.edu/archives/cipp-report-l.html>.