# THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 8 NUMBER 7

## JANUARY 2010
## AVIATION

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
Joseph Maltby

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHER
Liz Hale-Salice

Contact: CIPP02@gmu.edu
703.993.4840

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CENTER
for
INFRASTRUCTURE PROTECTION

This month's issue of *The CIP Report* concentrates upon the Transportation Systems Sector, specifically the Aviation Mode. This sector is a fundamental element in the daily lives of people and a valuable asset to the global market. Consequently, this sector is an ideal target for individuals and/or groups who wish to fracture and weaken the United States. The haunting memories of Pan American World Airways Flight 103, which were recently reawakened following the release of the convicted bomber; the devastating attacks on September 11, 2001; and the attempted bombing on Christmas Day 2009 all serve as reminders that the transportation system, particularly aviation, is vulnerable to terrorism.

The first article provides a general overview of the Transportation Systems Sector as well as the Aviation Mode within this sector. This article is followed by a brief discussion on the current and complicated challenges that surround airport passenger screening. Then, the Executive Director of the National Center for Critical Incident Analysis, Dr. Stephen Prior, examines the transmission of disease, including H1N1, through the aviation system. The next article focuses upon aviation and information security. Finally, Dr. Michael Romanowski, Director of the Federal Aviation Administration's NextGen Integration and Implementation Office, discusses the Next Generation Air Transportation System.

This month's *Legal Insights* examines the "Air Cargo Screening" Interim Final Rule. This Interim Final Rule was recently published in the Federal Register by the Department of Homeland Security, Transportation Security Administration.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP
George Mason University, School of Law

# An Overview of the Transportation Systems Sector: Aviation Mode

## Introduction

For thousands of years, civilizations have depended upon inventions such as the wheel and seafaring vessels to fish, hunt, travel to far off places, and transport goods. Therefore, the Transportation Systems Sector, established in 2003 by Homeland Security Presidential Directive 7, is vital to preserving our standards of living and economic security and stability. Consequently, the Transportation Systems Sector is an alluring target to individuals and/or groups who wish to disrupt the infrastructure of the United States.

The Transportation Systems Sector is divided into six modes of transportation: Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline. The Transportation Security Administration (TSA) is the Sector Specific Agency (SSA) for the Aviation, Mass Transit, Highway, Freight Rail, and Pipeline Modes. The United States Coast Guard is the SSA for the Maritime Mode. In addition to the SSAs, the Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC) work together to ensure that the vision of the sector is fulfilled.

### *Vision*

The vision of the Transportation Systems Sector is the realization of a "secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties."[1]

### *Mission*

The mission of the Transportation Systems Sector is "to continuously improve the risk posture of the Nation's transportation system."[2]

### *Goals*

According to the Transportation Systems Sector Specific Plan (SSP), the goals of the sector are as follows:

1) Prevent and deter acts of terrorism using or against the transportation system;

2) Enhance the resilience of the transportation system; and

3) Improve the cost effective use of resources for transportation security.

Since the establishment of the 18 critical infrastructure/key resources sectors, a critical component of the Transportation Systems Sector has been the Aviation Mode. However, while the tragic events of September 11, 2001 highlighted the need for improvements to aviation security, terrorism has been a threat to the aviation industry since the inception of commercial flights.

## Aviation

### *A Brief History of Aviation Security*

On May 20, 1926 the Air Commerce Act of 1926 was signed into law by President Calvin Coolidge. This historic legislation directed the Secretary of Commerce to "foster air commerce; designate and establish airways; establish, operate, and maintain aids to air navigation (but not airports); arrange for research and development to improve such aids; license pilots; issue airworthiness certificates for aircraft and major aircraft components; and investigate accidents."[3] Three days later, Western Air Express, a U.S. airline, offered one of the first regular passenger services from Los Angeles to Salt Lake City. However, shortly thereafter, it became evident that this exhilarating and novel mode of transportation could be used by some to promote their own agenda. In November 1955, a United Air Lines flight traveling from Denver, Colorado to Portland Oregon was destroyed by a bomb, killing all 44 passengers and crew. The son of a passenger on board the plane, J.G. Graham, was eventually arrested by

*(Continued on Page 3)*

[1] The Department of Homeland Security, Transportation Systems Sector Specific Plan, May 2007.

[2] Ibid.

[3] The Federal Aviation Administration (FAA), *FAA Historical Chronology, 1926-1996*, Updated December 1996.

**Aviation Overview** *(Cont. from 2)*

the Federal Bureau of Investigation for deliberately detonating the bomb. It was later revealed that Graham had hoped to collect the life insurance he had taken out on his mother. He was convicted and sentenced to death. In May 1961, a passenger on board a flight to Key West, Florida hijacked the plane and forced the pilot to fly to Cuba. According to the Federal Aviation Administration (FAA), this was the first in a series of hijackings in the United States. Almost ten years later, the copilot of an Eastern Air Lines shuttle was the first person to be killed during a domestic U.S. hijacking incident. The first passenger killed during a domestic U.S. hijacking occurred the following year, in 1971, when a passenger attempted to aid a stewardess who had been seized by the hijacker. On December 21, 1988, four days before Christmas, Pan American World Airways Flight 103 exploded near Lockerbie, Scotland. All 243 passengers and 16 crew members as well as 11 people on the ground were killed.[4] In 2001, one man was convicted of the bombing; however, in August 2009, he was released on compassionate grounds due to his terminal prostate cancer.[5] These past events demonstrate that the U.S. aviation industry was branded an appealing and vulnerable target prior to the tragic events on September 11, 2001.

> *Aviation Mode: Aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional public airfields. This mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.*
>
> -Transportation Systems Sector Specific Plan, May 2007

**Aviation Mode**

At 9:45 a.m. on September 11, 2001, in an unprecedented decision, the FAA grounded all U.S. air flights. By 12:15 p.m., over two hours after United Flight 93 crashed in Pennsylvania, the U.S. airspace was eerily quiet.[6] Almost ten years later, the TSA, the Department of Transportation, the FAA, the Department of Defense, the Department of Justice, airlines, airports, flight crews, air cargo industry members, State and local law enforcement, and perhaps most importantly, the passengers, continue to collaborate to ensure that the infrastructure of the aviation industry never again experiences an unplanned shutdown. These same groups also strive to fulfill the vision of the Aviation Mode within the Transportation Systems Sector. The vision of the Aviation Mode is to "achieve a secure, resilient, and efficient network of airlines; other aviation operators; airports; personnel; and infrastructure to ensure the safe and efficient movement of people and cargo and to prevent exploitation of the aviation transportation system to carry out attacks, while protecting the civil liberties of all individuals."[7] The components of the Aviation Mode include the National Airspace System; commercial airlines; commercial airports; general aviation; air cargo; and international programs (see page 20 for more information).

The three goals of the Transportation System Sector, listed in the introduction, are applied to the six modes, including aviation. In order to successfully achieve the first goal of the sector, which strives to prevent and deter acts of terrorism, the aviation mode created three objectives:

1) Implement flexible, layered, and unpredictable security programs using risk management principles;

2) Increase the vigilance of travelers and transportation workers; and

3) Enhance information and intelligence sharing among Transportation Systems Sector

*(Continued on Page 4)*

[4] The Federal Aviation Administration (FAA), *FAA Historical Chronology, 1926-1996*, Updated December 1996.

[5] The Department of Homeland Security, Transportation Systems Sector Specific Plan, May 2007.

[5] http://www.scotland.gov.uk/News/This-Week/Speeches/Safer-and-stronger/lockerbiedecision.

[6] The Federal Aviation Administration, Update to *FAA Historical Chronology: Civil Aviation and the Federal Government, 1926-1996*, Updated 1998.

[7] The Department of Homeland Security, Transportation Systems Sector Specific Plan, May 2007.

## Aviation Overview *(Cont. from 3)*

security partners.[8]

The first objective is met through the creation of programs such as the Federal Air Marshal Service, which President Obama recently expanded following the attempted bombing on December 25[9]; the Hazardous Materials Regulations; the Airport Liaison Agent Program, a program managed by the Federal Bureau of Investigation which assigns Special Agents to each TSA regulated airport; and the TSA National Explosives Detection Canine Team Program, a program that provides State, regional, and local law enforcement authorities with trained dogs. The second objective is met through appropriate investigations and security assessments of personnel as well as the Secure Flight Program, described by TSA as a "behind-the-scenes watch-list matching process that vets passengers against government watch-lists before a boarding pass is ever issued."[10] In an August 2009 press release, TSA stated that their goal is to vet 100% of passengers on domestic flights by early 2010 and 100% of passengers on international flights by the end of 2010.[11] At present, it is unknown if this program will be affected by the incident that occurred last December. The third objective, which urges for the enhancement of information and intelligence sharing among the Transportation Systems Sector, has always been an important issue; however, following the December 2009 attempted bombing, information and intelligence sharing has emerged as a top priority in the intelligence community and administration. On January 20, 2010, in a Senate Committee on Homeland Security and Governmental Affairs hearing, the Director of National Intelligence, Dennis C. Blair, and the Director of the National Counterterrorism Center, Michael E. Leiter, pledged to improve collaboration and information sharing.

In order to meet the second goal of the sector, which endeavors to enhance the resilience of the transportation system, the aviation mode has formed the following two objectives:

1) Mange and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability; and

2) Ensure the capacity for rapid and flexible response and recovery to all-hazards events.[12]

The personnel of the Aviation Mode work diligently to meet the first objective through programs such as the TSA's Transportation Security Operations Center, located at the Freedom Center facility, which gathers information from across the nation for the TSA. In addition, the FAA sponsors the Domestic Events Network, established after the terrorist attacks on September 11, 2001, which provides "timely notification to the appropriate authority that there is an emergency air-related problem or incident."[13] With regards to the second objective, according to the SSP, all Federal agencies are required to establish a continuity of operations (COOP) plan. COOPs are programs "designed to assure that the capability exists to continue essential agency functions in the event of an emergency."[14]

Finally, the objectives established to fulfill the third goal of the sector, which consists of improving the cost effective use of resources for transportation security, are as follows:

1) Align sector resources with the highest priority transportation

*(Continued on Page 18)*

[8] The Department of Homeland Security, Transportation Systems Sector Specific Plan, May 2007.

[9] Remarks by the President on Security Reviews, http://www.whitehouse.gov/the-press-office/remarks-president-security-reviews, January 5, 2010.

[10] http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm.

[11] http://www.tsa.gov/press/releases/2009/0812.shtm.

[12] The Department of Homeland Security, Transportation Systems Sector Specific Plan, May 2007.

[13] The Federal Aviation Administration, Air Traffic Organization Policy, (N JO 7210.724), http://www.faa.gov/documentLibrary/media/Notice/N7210.724.pdf, September 30, 2009.

[14] The Transportation Security Administration, TSA Management Directive No. 200.9, https://www.tsa.gov/assets/pdf/foia/TSA_MD_200_9_FINAL_071231.pdf, December 31, 07.

# Airport Passenger Screening

On December 25, 2009, a passenger onboard Northwest Airlines Flight 253 from Amsterdam to Detroit, Michigan, Umar Farouk Abdulmutallab, allegedly attempted to ignite an explosive device during the final descent into Metropolitan Airport. The attempted bombing has stimulated intense debates about the effectiveness of current aviation security policies and procedures, particularly terrorist watch-lists and airport passenger screening. This incident also reinforces concerns that the transportation system, particularly aviation, continues to be an appealing target to terrorists. Consequently, aviation security is once again preparing for microscopic examination.

On January 3, 2010, shortly after the attempted bombing, the TSA announced new security measures for international flights into the United States. Effective January 4, 2010, the TSA is mandating that "every individual flying into the United States from anywhere in the world who holds a passport issued by or is traveling from or through nations that are state sponsors of terrorism or other countries of interest will be required to go through enhanced screening."[1] The statement also authorizes the increased use of "enhanced screening technologies and mandates threat-based and random screening for passengers on U.S. bound international flights."[2] The TSA is not the only government agency that is calling for the enhancement of passenger screening. On January 7, 2010, President Obama, in his remarks about strengthening intelligence and aviation security, announced that his administration has increased the funding for homeland security and aviation security, which includes "more baggage screening, more passenger screening and more advanced explosive detection capabilities, including those that can improve our ability to detect the kind of explosive used on Christmas."[3]

At present, most travelers are familiar with the three-step passenger screening routine. The first step consists of the x-ray machine, where passengers place their carry-on luggage and loose items on the belt of the x-ray machine. Then, passengers are required to remove their shoes prior to step two, the walk-through metal detector. If the alarm is activated, passengers endure additional screening, which usually includes the hand-wand inspection and/or a pat down inspection. These are the steps that passengers have become familiar with during their domestic and international travels. Following the attempted bombing on Christmas Day 2009, these steps will most likely change over the next few years. However, travelers may be unaware that steps to improve aviation security were underway prior to this incident. In fact, the TSA has been evaluating and testing programs specifically related to passenger and baggage screening for several years. According to an April 2009 Congressional Research Service (CRS) report, programs that are being tested include "technologies for detecting explosives, including explosives chemical trace detection devices, whole body imaging systems, and advanced technology (AT) x-ray capabilities."[4]

So, what has been the delay in implementing these programs? According to the CRS report, policymakers and aviation security planners continue to disagree on security plans and strategies. In addition, while it is evident that security measures must be

*(Continued on Page 19)*

[1] The Transportation Security Administration, TSA Statement on New Security Measures for International Flights to the U.S., http://www.tsa.gov/press/happenings/010310_statement.shtm, January 3, 2010.

[2] Ibid.

[3] The White House, Office of the Press Secretary, Remarks by the President on Strengthening Intelligence and Aviation Security, http://www.whitehouse.gov/the-press-office/remarks-president-strengthening-intelligence-and-aviation-security, January 7, 2010.

[4] Bart Elias, Congressional Research Service, *Airport Passenger Screening: Background and Issues for Congress*, April 23, 2009.

# Tickets, Identification, Luggage, Bacteria, Viruses….

by Stephen Prior, Ph.D.
President, Therax, Inc. and Executive Director, National Center for Critical Incident Analysis

In the days following the first reports of the entry of swine flu (more correctly swine-origin influenza virus H1N1) into the United States last April, I was fortunate enough to lead a team that used advanced modeling and simulation tools to forecast the spread and possible impact of this latest challenge from Mother Nature. The tools were based on technologies developed at George Mason University (GMU) and provided a rapid forecast of how the swine flu would become the first pandemic in almost forty years and demonstrate how fast diseases can spread in the global community. In the ensuing months, the swine flu virus spread across the globe: by June 2009, the World Health Organization (WHO) confirmed that 74 countries had human cases, and in December, the WHO reported that over 200 countries had reported deaths from swine flu. In a sobering assessment of the problems associated with monitoring a disease that spread as widely as swine flu, the Director of the WHO noted that "it would take at least two years before a true death total is established." The transmission of diseases by contact between humans is as old as the human species; what has changed, most strikingly in the past five decades (during which air travel has increased at almost 9% per annum), is the rate of transmission or spread.

We are now facing, and in some cases are routinely exposed to, pathogenic (disease-causing) bacteria, viruses, parasites, fungi, and other assorted biological material that can travel vast distances in very short periods of time. Moreover, with the patterns of human movements that are now commonplace, the pathogens can 'leap' from country to country without necessarily exhibiting an uninterrupted trail. We can now be challenged by novel and emerging diseases with little or no notice of an impending public health problem.

Of the many transmission vectors that can spread disease, our infatuation with airline travel is an ongoing concern. The number of passengers (see box), the explosion in destinations, and the desire to visit 'exotic' locations around the globe mean that exposure to, transmission of, and susceptibility to an ever-increasing range of diseases has never been greater. Historically, before travel became commonplace, the average human was primarily exposed to diseases that were endemic to their locale and their limited social contacts. The initial contacts between villages has been replaced by the concept of a worldwide 'global village' where the hand that you shake — or who used the door handle prior to you — may have been on the other side of the globe just yesterday; and he or she may have been carrying more than just a passport, luggage, and some interesting holiday photos when they boarded the aircraft.

In 2008 air travel included:

- 4.874 billion passengers
- 51% of airports worldwide registered positive passenger growth
- Total aircraft movements was 77 million

The movement of disease with humans and the need to address the spread by interrupting the mechanisms of transmission has been a basis for public health response and has been documented since the 17th century when the Venetians imposed a forty day period (Italian: *quarenta*, the basis for the word quarantine) on ships visiting the port in an attempt to control the spread of the plague. Quarantines of people — voluntary or compulsory isolation — often raise questions of civil rights but their effectiveness in interrupting the transmission of disease is well established. Quarantine law in the

*(Continued on Page 7)*

Disease Transmission *(Cont. from 6)*

United States began in Colonial America in 1663, when in an attempt to curb an outbreak of the smallpox virus, the city of New York established a quarantine.

In recent years, the outbreak of SARS (Severe Acute Respiratory Syndrome, 2003), a disease with documented transmission by airline travelers, led to the imposition of both voluntary and compulsory quarantines. Interestingly, in the context of civil liberties, the SARS experiences demonstrated that voluntary quarantine was much more effective than the imposition of compulsory measures. Today, many airports (and sea ports) in the United States that provide points of entry for international travelers have quarantine stations (operated by the Centers for Disease Control and Prevention or CDC) but the concept of holding incoming travelers (and returning citizens) for forty days is not part of current thinking. In fact, even providing a temporary quarantining of all the passengers on an inbound aircraft from an infected country represents a significant logistical challenge as the size of aircraft increase and the daily rates of arrival continue to climb. Quarantine for travelers is now more likely to be a temporary hold in which diagnostic tests can be used, treatments offered, information on the disease provided, and data about the travelers collated to facilitate tracking as they continue their travels. The last quarantine under U.S. Federal law was imposed on Andrew Speaker in 2007 after he traveled to Europe and back while infected with drug-resistant tuberculosis. He was the first person since 1963 to be placed under Federal quarantine.

Allied to the imposition of public health measures to interrupt the spread of the disease or treatments for those potentially affected are the technologies for disease detection. These too have seen upgrades in recent years; the SARS outbreak in 2003 led to the widespread use of thermal imaging devices to 'screen' inbound (and more recently outbound) passengers on airlines. A similar screening was most recently used during the swine flu pandemic in 2009. The thermal devices provide a visual signal of an elevated body temperature that often accompanies infection with many pathogens. The fact that the elevation in temperature is often a very early indicator of infection and that many diseases are only spread during periods when the infected person is exhibiting an elevated temperature makes this type of screening an effective tool. It also provides a real-time 'diagnosis' that contrasts with many of the more specific tests for specific diseases; even those that claim to be 'rapid' may take several hours and complex equipment to provide the required results. Unfortunately, the swine flu outbreak showed that when the pathogen (H1N1 virus) is spread before a rise in temperature occurs, even a simple, real-time detection capability cannot halt the rapid spread of a disease around the globe.

So, how did the GMU modeling tools address the pandemic spread of swine flu? Interestingly, the answer lies in some simple principles that underlie disease transmission, some complex computational capabilities, access to a few key data sources, and an advanced modeling and simulation tool called MASON (www.cs.gmu.edu/~eclab/projects/mason).

MASON, a computer modeling tool conceived, designed, built, and maintained by GMU researchers, is a fast and discrete-event multiagent simulation tool designed to be the foundation for large custom-purpose simulations, and also to provide more than enough functionality for many lightweight simulation needs. MASON contains both a model library and an optional suite of visualization tools in 2D and 3D. Applications of MASON include complex adaptive systems, physical modeling, and abstract modeling. In the case of the modeling of the pandemic outbreak of swine flu, MASON provided the computational backbone to which three key components of a simulation could be attached and then linked to forecast future states of the disease as it spreads.

William Hamer and Ronald Ross pioneered the first component, a mathematical model for disease, in the early part of the twentieth century. Improvements to those early models included the development of 'compartmental models' that divide the exposed population into specific groups (compartments). One simple but effective version of such models provides a mathematical basis for transition between states describing

*(Continued on Page 8)*

Disease Transmission *(Cont. from 7)*

disease progression in individuals (and populations) as susceptible, exposed, infected, and recovered.[1] Using compartmental models and applying the observed features of the swine flu outbreak, the rate of disease progression and the periods for disease transmission could be calculated and used as inputs to the simulation.

The second component is tightly-coupled to the modeling of the disease characteristics and focuses on transmission between individuals (or groups) at specified locations. The modeling of this component provided a key decision-point for the simulation: high-fidelity modeling in which each individual and their respective contacts are modeled has been demonstrated but requires very large computational capability and can result in long run-times for the models. Modeling at the other end of the fidelity range, where large populations are considered as perfect mixing-bowls for the disease, are less computationally intensive but lack some important features that help to understand how diseases will spread. So, just like Goldilocks, the key is not too much, not too little, but just the right amount of fidelity to provide the required outputs for the model.[2] In the case of the early spread of swine flu in 2009, this meant modeling the major cities in Mexico, the United States, and Canada.

Lastly, the various geographic locations (and thus the populations at the locations) need to be linked as a network that is based on the probabilities that infected persons will mix with uninfected, susceptible persons. These probabilities can be calculated and included in the simulation using data on airline travel between the chosen locations in the network. These network considerations are particularly relevant in the study of the geographical spread of epidemics where the various long-range heterogeneous connections typical of modern transportation networks naturally give rise to a very complicated evolution of epidemics characterized by heterogeneous and seemingly erratic outbreaks, as recently documented in the case of SARS (www.who.int_csr_sars_en).[3] In this context, air-transportation represents a major channel of epidemic propagation. In fact, this publication demonstrated the use of the International Air Transport Association database to provide key inputs that correlated with global spread of infectious disease.

Through the linkage of the three components, the features offered in MASON, and some judicious decisions about what to model and at what fidelity, the early models for the 2009 swine flu outbreak were able to overcome the caution of George Box concerning modeling that '[a]ll models are wrong but some models are useful.' In this case, the useful models helped shape decisions about public health responses for a rapidly emerging novel disease that relied on air travel to move rapidly between distant geographic locations.

A glance back to the early days of air travel shows that this article is merely one of the latest in a line stretching back to the beginning of passenger travel. The January 23rd edition of *Flight* magazine in 1947 suggested that an international organization was needed to control the spread of diseases from endemic to non-endemic areas. The article further opined that '[t]he spread of disease can be held in check by a scheme which is internationally sponsored and internationally controlled.' Over 60 years have passed and, based on the events of 2009 with respect to swine flu, we now know that such high ideals are not feasible. But those same events of last year and the pioneering work at research centers like GMU are providing new tools that may help target the public health interventions that can slow or halt the spread of novel and emerging disease threats even as air travel expands to remote regions of the globe and our encounters with pathogens increase.

*(Continued on Page 22)*

[1] Bailey, Norman T. J. *The Mathematical Theory of Infectious Diseases and Its Applications*. (London: Griffin, 1975).

[2] Justin Lessler, James H. Kaufman, Daniel A. Ford, Judith V. Douglas, *The Cost of Simplifying Air Travel When ModelingDisease Spread* (2009).

[3] Vittoria Colizza, Alain Barrat, Marc Barthe´lemy, and Alessandro Vespignani, *The Role of the Airline Transportation Network in the Prediction and Predictability of Global Epidemics*. (2006).

# The Transportation Security Administration and Aviation Security

This winter, TSA experienced a busy holiday travel season bracketed by two security incidents, drawing significant attention to the challenges of aviation and information security, especially in the aftermath of the Christmas Day terror plot. These are the latest in a series of security and infrastructure protection concerns that have emerged in the last few months involving the Transportation Systems Sector, and more specifically, aviation.

In early December, the TSA released a copy of its airport screening procedures manual on the internet that was not properly redacted, allowing viewers to remove the protection of sensitive portions. The manipulation of this file was possible for anyone with a basic knowledge of Adobe Acrobat. According to the TSA, the manual was an outdated version, having been updated six times since its initial release, and was posted improperly by a contract employee. The document contained details about items which were not required to be screened, identified law enforcement credentials, and listed which countries' passports would lead to extra screening. It also noted how often baggage would be hand-screened and how procedures could be shortened during busy periods.

Critics both inside and outside Congress charge that these revelations make it significantly easier for terrorists to learn how to evade screening check points and potentially duplicate law enforcement credentials. Despite claims by the TSA that the information contained in the manual was outdated and therefore harmless, some argue that the screening process has not changed significantly enough for the document to be labeled as such. In a letter to the Secretary of the Department of Homeland Security, Janet Napolitano, members of the House Committee on Homeland Security inquired whether any legal action can be taken against websites which republish the manual. The TSA has investigated bloggers who posted copies of new screening procedure documents published in the wake of the Christmas Day terror plot, including searching their phones and computers, and has threatened serious consequences if the bloggers do not comply with a subpoena and reveal their source. The bloggers have argued that their posting of the material, which was unclassified, was not a security breach because it was sent by the TSA to every airline that serves the United States.

This incident was followed by a security breach in January 2009 when a passenger walked from the non-secure side to the secure side of a screening area in Newark Liberty International Airport to greet an arriving traveler. The airport terminal was shut down for hours while authorities re-screened thousands of travelers. The man in question was not found during the sweep. In addition, authorities were forced to review security footage of the airport recorded on security cameras operated by the individual airlines because the TSA cameras had been running but not recording during this period. They then discovered that this breach had taken place because the man had been left in line while the TSA officer left their post to deal with another traveler. The TSA employee has been placed on administrative suspension. The Port Authority Police have since arrested the individual believed to be responsible for the security breach.

At present, the TSA lacks a director. The nomination was stalled due to revelations that the nominee, Erroll Southers, made misstatements in a sworn affidavit to the Senate committee during the confirmation process about accessing confidential criminal records. Senator Jim DeMint of South Carolina also blocked the nomination because he wanted assurances that Southers would not advocate for collective bargaining rights for TSA employees. Some have argued that these breaches prove that the failure to confirm a TSA Director has made the United States less safe. Southers has since withdrawn his name from consideration. ❖

*(Continued on Page 22)*

# The Future of U.S. Air Traffic Control and Related Security

by Dr. Michael Romanowski
Director of NextGen Integration and Implementation Office
Federal Aviation Administration

In 2008, more than 800 billion passenger miles were flown in United States airspace.  For that to happen, more than 15,000 controllers provided service to America's 590,000 pilots, who flew 239,000 aircraft in and out of 20,000 U.S. airports.  However, our nation's air traffic control system, while providing extraordinary safety, is strained to efficiently handle this volume and is ill-equipped to handle our needs for the future.

To address these challenges, the FAA is leading a major initiative called Next Generation Air Transportation System, or NextGen, designed to revamp the nation's Air Traffic Control (ATC) system.  The overall goals of NextGen are to transform the ATC infrastructure from one that is largely rooted to inflexible and discrete ground-based, World War II era systems, into the realm of highly integrated, network-enabled, satellite-based technologies.  All major functions of ATC will be affected, including Communications, Navigation, and Surveillance (CNS).

To accomplish this transformation, the FAA is actively developing and deploying NextGen in partnership with other key government and civil sector stakeholders including; the Departments of Defense, Transportation, Commerce, and Homeland Security, NASA, the White House Office of Science and Technology Policy, and users such as airlines and industry groups.

A recognized and critical part of the NextGen transformation is Infrastructure Security and the general overall improvement to the security environment which will be brought about through the deployment of new systems and capabilities.  This has never been more important to the air traffic control system than it is now in a post 9-11 environment.  Security is therefore considered along every step of the way in the NextGen effort, from the formulation of new concepts of operation and system designs through development, testing, implementation, day-to-day operation, and in service support.

Managing an effort as complex as NextGen is a challenge that requires a multi-layered approach.  One key tool is the use of a structured approach called an Enterprise Architecture (EA), which provides Service and Infrastructure roadmaps describing how the FAA will evolve to NextGen.  The EA, along with robust portfolio management, is the "glue" which helps to integrate multiple programmatic activities into the delivery of a single, unified ATC system.  The EA includes Information System Security (ISS) Roadmaps that provide an enterprise wide security solution for the national airspace system.

Additional tools to address the security aspects of NextGen are handled through formal and disciplined processes that will guide the effort throughout its lifecycle. The FAA's Information Systems Security (ISS) process is being fully employed and is formalized as part of the agency's Acquisition Management System (AMS).  As programs progress through the AMS phases of Concept Development, Solution Implementation and In-Service Management, program managers are constantly challenged to consider and manage all aspects of information security management. Specific, rigorous processes requiring detailed assessments and documentation, such as Security Risk Assessment (SRA), Information System Security Plan (ISSP) and the Security Certification and Authorization Package (SCAP), must be accomplished to successfully complete the acquisition process and reach operational deployment. More importantly, as part of the FAA's Systems Engineering process, Information Systems Security Manager's (ISSM's) are employed to provide subject matter expertise,

*(Continued on Page 11)*

Next Generation *(Cont. from 10)*

oversight, and enforcement of security procedures throughout the lifecycle of NextGen systems.

The multifaceted nature of NextGen means that the security of the system will be addressed on several different fronts:

- In communications, several major changes are expected. The first involves improvements to air-to-ground communications, typically referred to as Data Comm. As the name implies, this change will move the FAA away from voice communications to digital data communications directly between pilot and controller, similar to text messaging. Data communications will automate repetitive tasks, and enable air traffic control to issue complex clearances (currently not possible) directly to pilots, providing precise instructions that can be clearly understood. This seemingly minor change will lead to significant efficiency and safety benefits. By moving away from sequential voice communications between pilots and controllers, large numbers of aircraft can be more effectively routed around weather cells, for example. Also, the decreased number of voice communications also will reduce radio frequency congestion and eliminate verbal miscommunication — a great safety improvement that will reduce operational errors. From a security perspective, it has the added benefit of providing a second direct communications means with the cockpit, which provides a level of redundancy that is not available today.

- The second major communications innovation currently being deployed is a new network-centric infrastructure known as System Wide Information Management (SWIM). It will connect the myriad of FAA systems that today require dedicated point-to-point connections which severely constrain the FAA's ability to get additional relevant information to the people who could use it most effectively to improve service delivery. SWIM is employing the current standards of a "publish and subscribe", Service Oriented Architecture (SOA), following industry best practices in the areas of governance and information security. When complete, SWIM will provide for sharing of information among diverse systems and increase common situational awareness, both on the ground and in the air. This will improve national and homeland security.

- In navigation, the FAA will move away from heavy reliance on ground-based aids to navigation, which causes pilots to fly circuitous routes from point-to point. Aircraft based Global Positioning System (GPS) satellite positioning will enable new Performance-Based Navigation (PBN) routes and procedures, allowing aircraft to fly more direct routes, that are tightly bounded both vertically and horizontally, which will save fuel and improve environmental performance. PBN also allows for the creation of more flexible routes into and out of high density airports, and provides the added security benefit from new tools for alerting controllers should an aircraft deviate from planned flight paths.

- In surveillance, the FAA will implement a new capability that is called Automatic Dependent Surveillance Broadcast (ADS-B). ADS-B uses aircraft based GPS position information to broadcast aircraft location and flight path information to ground stations and other aircraft. The ADS-B data will be fused with radar information in a national network, providing air traffic controllers with improved coverage and situational awareness. It can also provide surveillance in areas where it was previously not feasible, such as mountainous terrain. As an example, the FAA recently turned on "new" services across the Gulf of Mexico, where ADS-B ground stations were installed on oil platforms, providing coverage to over 240,550 square miles of airspace that could not see before. Improved surveillance coverage will provide significant security benefits. The nationwide infrastructure of ground-based ADS-B receivers and integration into the FAA's ATC displays will be in full operation by 2013.

Aside from increased security, the other enhancements provided by NextGen also reduce congestion, delay, distance flown, fuel burn, emissions, and noise. The ultimate goal is to provide benefits to the operators of all types of aircraft and, through them, to the traveling public. In reality, some of the NextGen improvements implemented in the past few years

*(Continued on Page 18)*

Legal Insights

# The Transportation Security Administration Interim Final Rule: Creating Private Sector Programs to Reach 100% Air Cargo Screening

by Shahin Saloom, J.D.

## Introduction

### *History of the Interim Final Rule*

On September 16, 2009, the TSA published an Interim Final Rule (IFR) entitled "Air Cargo Screening" in the Federal Register.[1] This IFR codifies a statutory requirement of the Implementing Recommendations of the 9/11 Commission Act[2] (the Act) that the TSA establish a system to screen 50% of cargo transported on passenger aircraft by February 2009 and 100% by August 2010. The implementing recommendations also mandate that this screening meet a level commensurate with that of passenger baggage, meaning screening at the piece level,[3] and the mandate is not accompanied by congressional funding, meaning that the private sector must pay for this increase in cargo screening. The IFR also mandates that aircraft operators ensure that 100% of cargo loaded onto their airplanes be screened by an aircraft operator, TSA approved cargo screening facility, or TSA itself.

The TSA determined it could not meet the 100% requirement by relying only on aircraft operators alone due to the sheer volume of cargo (12 million pounds per day) and the stringent chain of custody and security standards mandated in the implementing recommendations and therefore established, with this IFR, a program under which TSA can certify cargo screening facilities to screen all cargo destined for passenger aircraft, the Certified Cargo Screening Program (CCSP). The CCSP creates the option of secure screening earlier in the supply chain, away from the airport, with the intent that this will diffuse responsibility and cost throughout the supply chain, amongst shippers, freight handlers, and aircraft operators. TSA had been piloting the CCSP program at 18 U.S. airports that originate 96% of affected air cargo by validating over 200 facilities and is basically instituting this program nationwide.[4] The TSA hopes that enough facilities will become certified in the CCSP program to meet the 100% requirement by August 2010. This IFR became effective on November 16, 2009.[5]

### *Content of the Interim Final Rule*

The CCSP is designed to move more of the air cargo screening duties further back in the supply chain because the TSA has recognized that existing screening infrastructure simply will not be able to meet the burden of 100% screening by August 2010. This program therefore allows shippers, manufacturers, warehouses, distributors, logistic companies, and indirect air carriers to apply for and become Certified Cargo Screening Facilities (CCSF), effectively

*(Continued on Page 13)*

[1] 74 Fed. Reg. 47, 672.

[2] Pub. L. No. 110-53 sect. 1602, 121 State. 266, 478 (2007).

[3] TSA is concerned about lack of U.S. shipper's impact awareness about 100% screening issues (August 2010), http://www.tsa.gov/assets/pdf/ccsp_at_a_glance.pdf, June 5, 2009.

[4] U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, "100% Air Cargo Screening: Can We Secure America's Skies?", Statement of Edward Kelly, General Manager, Air Cargo Transportation Sector Network Management, http://homeland.house.gov/SiteDocuments/20090318144700-36589.pdf, March 18, 2009.

[5] 74 Fed. Reg. 47, 672.

**Legal Insights** *(Cont. from 12)*

distributing the burden throughout the supply chain. CCSF candidates must submit an application for each candidate facility to the TSA and must also provide a TSA-approved validator's evaluation of their security measures.[6] The IFR also contains the requirements and processes for that application and validation, as well as the requirements and processes for firms and individuals that wish to become TSA-approved validators.

CCSFs must naturally use TSA-approved security methods and standards and must also appoint security coordinators and alternates with 24/7 availability and ensure that all of these security coordinators, their alternates, facility managers, and any employees or authorized representatives that screen or have access to cargo undergo a TSA-conducted Security Threat Assessment (STA). In summary, the IFR creates a program that enables off-airport entities to become TSA-certified cargo screeners, and defines the scope, duties, responsibilities, operating procedures, and security and compliance benchmarks for that program.

## Criticisms of the CCSP

This rule was promulgated as an IFR without notice and public comment but the TSA did invite interested parties to submit written comments to this rule for the record. The IFR creates an entirely new program, the CCSP, which will be the exclusive option for the private sector to continue to screen air cargo. Not only does the rule contain rigid screening, security, and compliance requirements but it does not provide any funding for any of these mandates. The rule also introduces an entirely new private sector certification function that acts as a watchdog of participants in the CCSP for the TSA. Such a complete upheaval of an industry in anticipation of a drastic increase in cost, workload, and responsibility naturally engaged the industry in contemplating the actual implications of this rule. The following criticisms arise directly from the individuals most affected by the rule: the private sector actors that the TSA hopes will populate this new program.

*Cost of Reaching 100% Screening*

The TSA has expressed concern that several factors that led to the relative ease with which the 50% screening level was reached encouraged complacency in the cargo supply chain.[7] The TSA notes that the pending economic recovery could drastically exacerbate the efforts to reach 100% screening because screening 100% of 15 million pounds per day (projected return to 2007 levels due to economic recovery) in 2010 actually represents at 300% increase in cargo screening from screening 50% of 9 million pounds per day in February 2009.[8] The TSA is also concerned that the 50% level was reached by concentrating on cargo already at the piece level and that screening of the consolidated, "palletized" cargo (that may frequently require timely and costly repacking) lies ahead.[9]

This large increase of the burden on the private sector screening capabilities did not escape the notice of the various firms and associations that commented on the rule. The Airforwarders Association (AA) estimated that it would cost between $50,000 and $500,000 per facility for new screening technology and that these costs will force smaller potential CCSP candidates out of the program, leading to consolidation of the market which will lower competition and lower the chance of meeting the 100% screening deadline.[10] Especially in light of the 25% decrease in cargo volume, the AA is joined by several other stakeholders in requesting government funding in the form of tax incentives for equipment purchases.

These cost projections take for granted the availability of appropriate screening technology but several parties commented on

*(Continued on Page 14)*

[6] National Air Transportation Association, White Paper – Air Cargo Screening Interim Final Rule, http://www.nata.aero/data/files/g%20&%20i%20affairs/airline%20services%20council/1009aircargosecnprm_wp_asc.pdf, November 6, 2009.

[7] Ibid³.

[8] Ibid.

[9] Ibid.

[10] Ibid⁴.

**Legal Insights** *(Cont. from 13)*

the lack of appropriate technology. The International Air Cargo Association (TIACA) noted in their comments that current TSA certification of equipment is too heavily focused on the screening of passenger baggage and that the TSA should therefore expedite their efforts in identifying, testing, and certifying more appropriate technologies.[11] They also urge the TSA to use the $4 million appropriated for skid and pallet cargo screening technology in the 2010 Homeland Security Appropriations Act as quickly and transparently as possible,[12] and that Congress increase their funding for canine screening as a stopgap measure.[13]

Potential members of the CCSP also recognized other unsupported costs of the program, including warehouse facilities, training and certification, and the maintenance of a complex compliance relationship with the TSA[14] including the fact that a CCSF applicant would have to pay the fee of the third party validator. The AA, worried that their members as CCSF applicants would have to pay validation fees despite a 25% drop in cargo volume, recommends that TSA control and limit validation fees and include enough time in their process to collect and analyze public comment.[15] They also recommend that the TSA certify a large number of validators to meet the forecasted demand as applications to the CCSP increase. The combination of these costs, for new equipment, facilities, training, and compliance struck some firms as prohibitive.[16] In fact, many of the comments referenced a finding by the Government Accountability Office (GAO) from March of 2009 that the entry costs of the CCSP would force 80% of small freight forwarders out of business,[17] and claimed that the IFR did not change the cost conditions sufficiently to alter the GAO's determination.

*Security Threat Assessment Requirement*

The IFR also requires that any employee, supervisor, or manager that screens cargo or has unrestricted access to the cargo at any point in the chain of custody undergo a TSA Security Threat Assessment (STA). Many of the stakeholders in this field have been operating under stringent security standards already and apply this perspective to their criticism of this new certification program.

For example, the Express Association of America (EAA) notes that the requirement of an STA for affected employees is only a futile distinction because, in smaller firms, it is very hard to internally segregate employees that handle cargo within a facility from those that do not,[18] and this requirement realistically leads to a costly facility-wide certification. The National Air Transportation Association (NATA) also makes the point that the requirement, as articulated, is not as costly or redundant as its application in the real world because many of the individuals screening cargo who would have to undergo CCSP STA will have already gone

*(Continued on Page 15)*

[11] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Susan Presti representing The International Air Cargo Association, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a5837f, November 16, 2009.

[12] Ibid.

[13] Ibid[4].

[14] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Fernando Soler representing SOS Global Express, Inc. http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a5838b, November 16, 2009.

[15] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Brandon Fried representing the Airforwarders Association, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a57fe7, November 16, 2009.

[16] Ibid.

[17] U.S. Government Accountability Office, GAO-09-422T, "Preliminary Observations on TSA's Progress and Challenges in Meeting the Statutory Mandate for Screening Air Cargo on Passenger Aircraft" March 18, 2009.

[18] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Michael C. Mullen representing the Express Association of America, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a48faa, October 22, 2009.

**Legal Insights** *(Cont. from 14)*

through an STA to obtain airport identification.[19]

TIACA notes another weakness in the STA requirements in the five year reapplication requirement. This vetting resolution is not fine enough for security purposes; TIACA recommends a more organic process in which all information on STA applicants is continually cross-checked with the various terrorist and law enforcement databases that TSA uses in the initial STA, rather than a binary update every 5 years.[20] The Air Line Pilots Association (ALPA) notes a similar weakness in the STA program by comparing the TSA STA program to the security requirements of cargo handlers at an airport.[21] An airline employee who handles cargo at the airport is subject to fingerprint-based criminal record check while an employee with the same access at an off-airport CCSF need only be vetted by name-based STA. ALPA cites two studies that show that approximately 10% of fingerprint "hits" do not match the corresponding name on the submission, meaning name-only systems let some people through, and therefore recommend both finger-print based criminal record checks and the TSA STA for CCSF cargo screening personnel.

*TSA-Approved Validators of CCSP Applicants*

Perhaps the most troubling aspect of the IFR to industry stakeholders is the creation of TSA-approved validators of CCSP applicants. The IFR contains the necessary requirements an individual must possess to become a validator, describes the role of a validator in validating CCSP applicant security measures, and places certain restrictions on the interaction between validators and the facilities they validate. The creation of an unfunded mandate on the private sector is nothing new and the complaints over cost, technology, and certification outlined above are all, while valid, predictable and foreseeable when a federal bureaucracy attempts to define a new program. The introduction of a private sector third party validator that acts as a gatekeeper and compliance agent for the TSA, however, was a completely new development and engendered a broad range of criticism. Several stakeholders criticized the restrictions and conditions placed upon the relationship between validators and CCSP applicants. As no fee for the validation was specified in the IFR and the applicant must pay the fee to complete their application, the applicant CCSF basically pays the validator for access to the program, creating a conflict of interest.[22] The IFR also prohibits validator firms from directly marketing their assessments, leading to competition based on price alone. BIVAC notes that a similar program in France's cargo screening system led to price undercutting and eventual compromised assessments and therefore recommends that the TSA set a price floor on the validations to instigate some competition based on performance.[23]

Concerns over competition in the newly created industry of CCSP validation firms also motivates TIACA concerns that there simply will not be enough validators, due to the high burdens of entry (the necessary qualifications and experience are very high, leading to

*(Continued on Page 16)*

[19] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Michael France representing the National Air Transportation Association, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a5652b, November 12, 2009.

[20] Ibid[11].

[21] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Greg Bergner representing the Air Line Pilots Association, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a57f31, November 11, 2009.

22 U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Peter A. Quinter representing Becker & Poliakoff, http://www.regulations.gov/search/Regs/home.html #documentDetail?R=0900006480a3c234, October 5, 2009.

[23] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Satiam Khadar representing BIVAC North America, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a571a0, November 13, 2009.

Legal Insights *(Cont. from 15)*

a high cost of recruitment and high labor costs), to create enough price competition in the market to drive prices down, and that potential CCSP applicants will therefore not apply due to high validator costs.[24] TIACA notes that these economic pressures leading to a small number of small validation firms also discourages CCSF applicants due to concerns about private information; potential applicants will not risk being validated by the same firm that validated a rival.[25] Industry stakeholders have even taken issue with the measure the TSA proposed to address potential conflicts of interest; that validation firms may not perform more than two validations of the same firm, for the externalities it creates. This policy results in fairly high marketing costs for validation firms due to the restrictions on repeat business. Add this limited marketing ability to the high operating costs due to the strict requirements on labor and a restricted potential market (after the initial rush to meet CCSF certification ahead of the 100% requirement deadline) and validation firms will not have the steady flow of business that most other service firms rely on in the private sector.[26]

***Delegation of Federal Responsibilities***

These concerns led to several industry stakeholders criticizing the delegation of security functions to the private sector. NATA notes that the IFR includes the TSA inspection of CCSFs every 36 months and therefore the requirement of an external validation every 36 months as well is merely redundant. NATA considers the entire validation program an inappropriate delegation of governmental oversight to the private sector because shifting cost to the private sector does not create a commensurate benefit in light of the redundancy of the private program.[28] The EAA also criticizes the TSA for the use of third party validators because they also consider the validation of a private sector company's strict compliance with a government-mandated and defined security program to be a government function.[29] Validation standards cannot be as universal with many private firms as it could be with one validator, the TSA. ALPA also believes that the TSA has gone too far in delegating oversight and vetting authority to an outside entity and may not have reduced their compliance burden with the addition of an outside agent.[30] The TSA must still monitor the education, oversight compliance, and consistency of application and interpretation of the validators. This remaining compliance burden, in addition to the potential conflicts of interest in the approval process and the lack of certainty in the STA vetting process, led ALPA to join NATA and the EEA in calling for a more robust federal role in certifying CCSFs.

Several stakeholders have gone even further and called for the Federal government to re-evaluate the exclusive role of the private sector in cargo screening. The AA claims that the TSA's mission is to secure borders but also maintain the flow of commerce and is therefore against the concept of 100% screening when compared to the TSA's other risk-based security programs which do not treat every item as the same potential threat level.[31] When compared to a risk-based security program, the 100% screening requirement is both less cost effective, and may make us less safe.

The lack of adequate security measures led SOS Global Express (SOSGE) to claim that the CCSP cannot meet the security standards required by the Act to provide a level of screening commensurate

*(Continued on Page 21)*

[24] Ibid[11].

[25] Ibid[11].

[26] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Steven G. Ballard representing Cargo Compliance Group LLC, http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a58339, November 15, 2009.

[27] Ibid[19].

[28] Ibid.

[29] Ibid[18].

[30] Ibid[21].

[31] Ibid[4].

# The Relevance of Risk Management and Information Sharing to Homeland Security

## One-Day Conference

## February 10, 2010

at

George Mason University - Arlington Campus
Original Building, Room 329
3401 Fairfax Drive
Arlington, VA 22201

Click *Here* to *Register*, view *Agenda*, find out *Transportation Options*, and view *Fees*.

Co-hosted by:

George Mason University | School of Law
Center for Infrastructure Protection

SARMA
Security Analysis and Risk Management Association

Sponsored by:

PriceWaterhouseCoopers

Next Generation *(Cont. from 11)*

are already providing significant benefits.

Early this year, the FAA will publish its annual NextGen Implementation Plan. This plan reports on all the goals and milestones the agency intends to achieve in the next few years and through the end of 2018 (the mid-term phase). The report will be available on the FAA's NextGen web site at http://www.faa.gov/about/initiatives/nextgen and additional information on NextGen is available at this site. ❖

**Aviation Overview** *(Cont. from 4)*

security risks using both risk and economic analysis as decision criteria;

2) Ensure robust sector participation as a partner in developing and implanting public sector programs for critical infrastructure/key resources protection;

3) Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts; and

4) Align risk analysis methodologies with the Risk Analysis and Management for Critical Asses Protection (RAMCAP) criteria outlined in the National Infrastructure Protection Plan.[15]

Following the events on December 25, 2009, aviation security is being carefully scrutinized by government agencies and policymakers. The goals and objectives that have been established by the Transportation Systems Sector will most likely be refined to address the ongoing and emerging aviation security threats. In the upcoming months, the TSA will work with its public and private partners to improve aviation security. As the aviation industry continues to transport people and goods around the globe, it is essential to strengthen the goals and objectives of the Transportation Systems Sector, particularly within the Aviation Mode. ❖

[15] The Department of Homeland Security, Transportation Systems Sector Specific Plan, May 2007.

Passenger Screening *(Cont. from 5)*

improved, policymakers and aviation security planners, especially the TSA, are plagued with multiple challenges. Some of these challenges include planning for the inevitable increase in "passenger traffic" and "wait times;" developing effective technologies to detect explosives and bomb-making components whilst avoiding the invasion of privacy; and managing funds appropriately and effectively.[5] The preservation of privacy has been a particular challenge to aviation security planners. In particular, the whole body imaging technology, which has the capability to reveal private, sensitive areas and prosthetics, has been criticized by organizations such as the American Civil Liberties Union and the Electronic Privacy Information Center. These organizations claim, for various reasons, that the implementation of this technology is an invasion of privacy by a machine that may or may not be effective in detecting weapons, simulated explosives, and components of devices.[6] According to the TSA website[7], this technology remains optional for passengers. However, recent media reports are brimming with predictions that this technology will ultimately become mandatory. A recent USA Today/ Gallup poll, which the TSA links to on their website, indicates that air travelers approve of installing this technology at airports. According to the poll, 78% of respondents approve of using the scanners.[8] Whether or not air travelers maintain this sentiment remains to be seen. Regardless, the debate about new technologies and effective security measures will continue to intensify.

On January 27, 2010, Representative Bennie G. Thompson, the Chairman of the U.S. House of Representatives Homeland Security Committee, will hold a hearing on the incident that occurred on December 25. Prior to this hearing, on January 8, Chairman Thompson sent a letter to President Barack Obama which called for increased information sharing, refinement of the terrorist watch-list, careful review of screening technology, including the controversial whole body imaging, and protocols, and swift confirmation of leadership vacancies in the U.S. Customs and Border Protection, the TSA, and Office of Intelligence and Analysis. This letter is most likely a foreshadowing of the issues that will be discussed at the January 27th hearing. The Senate Committee on Homeland Security and Governmental Affairs, led by Senator Joseph E. Lieberman (ID-CT), Chairman, and Senator Susan M. Collins (R-ME), Ranking Member, held two hearings about the Christmas Day Attack on January 20, 2010 and January 26, 2010. In addition, the Director ofNational Intelligence, Dennis C. Blair, is also investigating the December 2009 terror plot. Director Blair has requested John E. McLaughlin, former Acting Director of the Central Intelligence Agency, to review the intelligence communications leading up to this event. Needless to say, during the next several months, a plethora of reports will be released regarding the attempted bombing.

So, will the friendly skies continue to welcome travelers and evolve into a safer environment? While changes in aviation security are inevitable, at present, it is too soon to forecast what and how effective these changes will be for air passengers. Considering the significance of the infrastructure of the aviation industry to the United States, hopefully these changes will be both effective and amenable to passengers. ❖

[5] Bart Elias, Congressional Research Service, *Airport Passenger Screening: Background and Issues for Congress*, April 23, 2009.

[6] Ibid.

[7] http://www.tsa.gov/approach/tech/imaging_technology.shtm.

[8] http://www.usatoday.com/travel/flights/2010-01-11-security-poll_N.htm.

## Components of the Aviation Mode

**National Airspace System** (NAS): NAS is the dynamic network of facilities, systems, regulatory oversight, services, airspace, and routes that supports flights within U.S. airspace, including the international airspace delegated to the United States for air navigation services. FAA regulates and operates this service.

**Commercial Airlines**: Commercial airlines are regularly scheduled or public charter operations that are regulated under Title 49 of the Code of Federal Regulations (CFR). The regulations apply to both domestic and international operations flying within, from, to, or over the United States. Although commercial operations typically use large transport category aircraft, any type of aircraft—from a piston single-engine aircraft to an intercontinental jet—may be used.

**Commercial airports**: Commercial airports are defined as airports with regularly scheduled commercial passenger service. Currently, there are approximately 450 commercial airports in the United States that utilize TSA screening resources. The network of civilian and civilian/military joint-use airports is clearly perceived to be an essential resource for the Nation's economic and psychological well-being. Airports are also symbolic of U.S. citizens' expectations of freedom of travel, and are increasingly becoming nodes at which many or all modes of transportation interface.

**General Aviation** (GA): GA is defined as all segments of the aviation industry other than regularly scheduled commercial air carriers and military aviation. GA's 200,000 aircraft and 630,000 certificated pilots transport 145 million passengers each year and use some 19,000 landing facilities. The GA industry encompasses a wide range of activities, from pilot training to flying for business and personal reasons, charter operations, delivering emergency medical services, firefighting, law enforcement, and sightseeing. Operations range from short-distance flights in single-engine light aircraft to long-distance international flights in corporate or privately owned "wide-bodies" and from emergency aero-medical helicopter operations (i.e., MEDEVAC) to air-ships hovering over open-air sporting events.

**Air Cargo**: Air cargo is defined as property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. U.S. mail is not considered cargo and is covered under a separate security program.

**International Programs**: The TSA International Programs Office is an integral, but unique part of the intricate web protecting the U.S. civil aviation system. The International Programs Office protects international civil aviation at the point of origin en route to the United States or in select upstream locations, with the goal of ensuring freedom of civil aviation operations for people and commerce. The International Programs Office also provides global quality control for civil aviation security and assists in improving the international level of security through maintaining effective business processes for assessments, surveys, air carrier inspections, crisis response, and management, combined with dynamic strategic, tactical, and operational planning.

*-Transportation Systems Sector Specific Plan, May 2007*

**Legal Insights** *(Cont. from 16)*

with passenger cargo as currently configured, and that the IFR does not justify their position that the CCSP will indeed meet these security requirements or state how.[32] They claim that chain of custody protections are not robust enough and that moving screening to an earlier point in the supply chain increases exposure to tampering. They also note that the IFR does not address the concerns of the March 2009 GAO report that found that it would be unlikely that enough firms will join CCSP to meet security standards and that the technology has not been identified and approved to allow scanning at the piece level.[33] SOSGE is joined by Samuel Shapiro and Company in recommending that these cost and security concerns dictate that CCSP must be a compliment to, rather than a substitute for, a federal air cargo screening program operated by the TSA at all American airports.[34] They claim that this hybrid system will allow thousands of mid-size freight forwarders to stay in business and is the only way to get enough screening capacity to meet the 100% screen ng mandate.[35] ❖

[32] Ibid[14].

[33] Ibid.

[34] U.S. Department of Homeland Security/Transportation Security Administration, Interim Final Rule on Air Cargo Screening, Comment of Elizabeth K. Grant representing Samuel Shapiro & Company, Inc., http://www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480a59575, November 13, 2009.

[35] Ibid[14].

## Security Incidents *(Cont. from 9)*

### References

Brian Ross & Matt Hosford, "Massive Security Breach As Agency Gives Away Its Secrets," ABC News, December 8, 2009, http://abcnews.go.com/Blotter/massive-tsa-security-breach-agency-secrets/story?id=9280503.

Bennie Thompson & Peter King, Letter to Secretary Napolitano, December 9, 2009, http://www.fas.org/sgp/congress/2009/hsc120909.pdf.

Robert O'Harrow Jr., "TSA Nominee Misled Congress About Accessing Confidential Records," *The Washington Post*, January 1, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2009/12/31/AR2009123102257.html.

"Thousands Rescreened at Newark Airport," *CNN*, January 4, 2010, http://www.cnn.com/2010/US/01/04/new.jersey.airport.breach/index.html?iref=allsearch.

## Disease Transmission *(Cont. from 8)*

Passenger screening, rapid diagnosis, modeling and simulation will all contribute to trying to limit the next outbreak of an emergent or re-emergent disease and GMU will play its part. Of course, one alternative would be to limit travel, particularly travel for leisure pursuits, but no one would take that suggestion seriously, even if the next pandemic is more severe than this one. Or would they? ❖

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1