THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 11 NUMBER 7

JANUARY 2013

AVIATION

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

This month, *The CIP Report* examines the aviation subsector. One of six Transportation Systems Sector modes, aviation includes commercial aircraft, airports, and air traffic control systems, as well as civil and joint use military airplanes, airports, and seaplane bases. Essential to our Nation's economy and an obvious terrorist target, our authors shed light on some unique aspects of this subsector.

GEORGE MASON UNIVERSITY
School of Law

CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, Brian Legan and Christopher Kelly of Booz Allen give us an introduction to civil aviation infrastructure, highlighting emerging technologies and potential threats. Then, Robert Coullahan and Robert Desourdis discuss unmanned aircraft systems and public safety. Dave Buczek subsequently explains the risks of aviation operation fatigue and offers guidance on how to manage it. Next, ProPublica's Michael Grabell evaluates the declining use of body scanners in major airports across the Nation. Finally, in this month's *Legal Insights*, Aviation Law Professor Greg Walden makes the case for grant-free airport infrastructure funding.

We would like to take this opportunity to thank the contibutors to 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
Director, CIP/HS
George Mason University, School of Law

Civil Aviation Infrastructure: Protecting a System-of-Systems

by Brian M. Legan, Vice President and Christopher Kelly, Senior Vice President
Booz Allen Hamilton, Inc.

Introduction

Homeland Security Presidential Directive (HSPD)–7 designates the air traffic control (ATC) system as part of the Nation's critical infrastructure due to the important role civil aviation plays in commerce and the safety and mobility of people. This designation requires the Secretary of Transportation and the Federal Aviation Administration (FAA) to ensure that the ATC system and related systems are protected from both physical and cyber security threats to prevent disruptions in air travel.

The "Bricks and Bytes" of Our Aviation Infrastructure

An appreciation of the enormity and complexity of our U.S. National Airspace System (NAS) is essential to fully grasp the challenge of protecting critical aviation infrastructure. The NAS is the largest and safest in the world, accommodating an average of 60,000 flights per day (or over 35% of air traffic worldwide) and over 750 million passengers each year. The unparalleled aviation safety record in the United States is dependent upon a massive, distributed array of critical infrastructure components: over 600 air traffic control facilities, 450 commercial airports, 19,000 airfields, and over 64,000 communication, navigation, surveillance, and automation components and related infrastructure.[1] This array of facilities, systems, and equipment ultimately enables people—over 15,000 air traffic controllers, 6,000 technicians, and 5,000 aviation safety inspectors[2]—to safely and effectively manage an air traffic system that contributes over $1 trillion annually to the national economy.

In addition to this physical infrastructure (the "bricks"), the Next Generation Air Transportation System (NextGen) will rely upon an information architecture that spans the entire enterprise, employing network-centric "cloud" capabilities and the digital exchange of mission critical information (the "bytes") provided by space-based and aircraft-based sources. The FAA's NextGen Implementation Plan illustrates that success hinges upon building an integrated system-of-systems composed of advanced Communication/Navigation/Surveillance (CNS) infrastructure, automation, and avionics capabilities and a concurrent evolution in policy, airspace design, and workforce competencies.[3] The migration from ground-based navigation and surveillance to space-based and aircraft-based systems is already in progress, including a phase-out of some legacy systems and a phase-in of new capabilities. The FAA is increasingly reliant upon commercial satellite systems to provide essential services including communication, navigation, remote sensing, imaging, weather, and meteorological support. For example, systems such as Automatic Dependent Surveillance Broadcast (ADS-B) provide more precise position, navigation, and timing information to allow pilots and controllers to enable efficient arrivals and departures from airports and preferred trajectories en route. ADS-B uses Global Positioning System (GPS) information to provide continual broadcast of aircraft position, identity, velocity, and other information over *unencrypted* data links to generate a precise air picture for air traffic management.

(Continued on Page 3)

[1] FAA Administrator's Fact Book, June 2012.
[2] Ibid.
[3] FAA. 2012. NextGen Implementation Plan. FAA, March 2012.

(Continued from Page 2)

system that distributes information using commercial air-to-ground digital data link networks to connect FAA air traffic control (ATC) sites and DataComm-equipped aircraft.

As traffic volume and complexity increase, system wide information management (SWIM) will also be critical to the continued safety and efficiency of air traffic management. There is an increasing use of commercial software, Internet Protocol (IP) technologies, and web-based applications to assimilate and distribute information from a variety of sources to support ATC services. Common IT communication protocols and commercial-off-the-shelf (COTS) equipment are also being used on newer aircraft at unprecedented levels. This evolving service-oriented architecture will eventually migrate aeronautical information to a digital, cloud environment. Both aircraft and air traffic control systems will serve as "nodes" in a vast network of federated systems, supported by a range of standards-compliant and interoperable applications, running on a variety of platforms.[4]

Challenges and Opportunities

The implementation of the NAS enterprise architecture, network-centric ATC operations, and SWIM improves resilience and adds flexibility for continuity of operations This evolving system architecture, for example, provides increased agility for mitigating planned and unplanned disruptions by allowing the seamless transition of information and operations to alternate sources and locations. Conversely, as our aviation network increasingly relies upon the digital exchange and sharing of information among diverse constituents (e.g., air traffic control, pilots, DoD, DHS, international airlines, third-party consumers) using various devices and applications, we become susceptible to new threats. These emerging threats may be from malicious actions, unintended interactions, or natural events. The migration from legacy, stove-piped ATC systems to an interconnected *system-of-systems* brings new challenges and considerations for critical infrastructure protection.

To date, critical infrastructure protection efforts and investments have been largely focused on protecting *physical* aviation assets. For example, passenger and baggage screening, explosive detection, video surveillance, biometrics and identity verification measures, facility access control systems, and related efforts have been the subject of intense development and debate since the formation of the Department of Homeland Security (DHS) and Transportation Security Administration (TSA) a decade ago. While these physical infrastructure protection measures are logical imperatives, they do not address the coincident and growing threats to our aviation system's critical *cyber infrastructure*. We must recognize that our air transportation system is not immune to similar disruptions that have already been seen in the banking, financial, and healthcare industries.

Evolving Nature of Vulnerabilities and Threats

Gen. Keith B. Alexander, head of the National Security Agency (NSA) and the United States Cyber Command, cited a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011. He also acknowledged an increase in foreign cyber attacks on the United States aimed at critical infrastructure and rated our preparedness to defend against a major attack as a "3" on a scale of "1" (unprepared) to "10" (fully prepared).[5]

There have been several reports published recently that highlight the vulnerability of our evolving air transportation cyber infrastructure. The USDOT Inspector General audited 70 FAA web-based applications including systems that disseminate information over the Internet, such as communications frequencies for pilots and and controllers, plus other internal applications used to support ATC systems. The results of these tests revealed over 3,800 vulnerabilities—including more than 750 high-risk

(Continued on Page 12)

[4] Civil Air Navigation Organization (CANSO). 2012. "Global Ambition: ICAO Navigation Conference Calls For Alignment." *Airspace–Journal of the Civil Air Navigation Organization*. Issue 19, Quarter 4, CANSO, 2012.

[5] Sanger, David, and Eric Schmitt. 2012. "Rise Is Seen In Cyber Attacks Targeting U.S. Infrastructure." *The New York Times*, July 26.

Planning Considerations for Unmanned Aircraft Systems Deployment in the Public Safety Mission

by Robert J. Coullahan, CEM, CPP and Robert I. Desourdis, Jr.*

Recent policy guidelines promulgated for the use of Unmanned Aircraft Systems (UAS), and the FAA initiative to solicit proposals for UAS Test Sites across the Nation, are among a confluence of program and policy developments that will impact public safety capabilities and operational deployment opportunities in the near future. As we adapt to and integrate this very capable technology into civilian applications, it is imperative that public safety agencies understand the planning considerations that accompany the fielding of these life-saving UAS systems.

UAS refers to systems whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. It is a broader term that includes equipment, networks, and personnel in addition to Unmanned Aerial Vehicles (UAVs). UAS come in a wide range of shapes and sizes designed for diverse applications. They may have a wingspan as large as a Boeing 737 or be smaller than a radio-controlled model aircraft. Regardless, a designated pilot in command is always in control of a UAS. In the United States alone, the FAA reports that approximately 50 companies, universities, and government organizations are developing and producing over 155 unmanned aircraft designs.[1] As an example of the maturity of their operational use, the DoD possesses an unmanned aircraft inventory that increased more than 40-fold from 167 aircraft in 2002 to nearly 7,500 in 2010. In November 2010, unmanned systems achieved one million combat hours. In its recently published Roadmap for UAS, the DoD identified milestones for the integration of UAS technologies and capabilities in the airspace, as shown in **Figure 1**.[2]

Figure 1 Milestones for Airspace Integration

(Continued on Page 5)

[1] Federal Aviation Administration, Fact Sheet – Unmanned Aircraft Systems (UAS), Updated July 2011, Washington, D.C.

[2] U.S. Department of Defense, Unmanned Systems Integrated Roadmap: FY2011-2036, Reference Number: 11-S-3613, October 2011,

(Continued from Page 4)

Historically, UAS have supported military and security operations overseas, with training occurring in the United States. In addition, UAS are utilized in U.S. border and port surveillance by the DHS, scientific research and environmental monitoring by the National Aeronautics & Space Administration (NASA) and the National Oceanic & Atmospheric Administration (NOAA); public safety by law enforcement agencies, research by state universities; and various other uses by public (government) agencies. Interest is growing in civil uses, including commercial photography, aerial mapping, crop monitoring, advertising, communications, and broadcasting. Unmanned aircraft systems may increase efficiency and cost effectiveness of operations while at once enhancing safety and perhaps saving lives.

With more than 18,000 domestic law enforcement agencies in the United States and many more public safety agencies, including fire service and emergency response teams, the potential demand for aviation assets is high. Based upon various studies over the years, it is believed there are less than 400 law enforcement aviation units. Thus, less than 3% of all law enforcement organizations have aviation assets to support their daily operations. This is reflective of the cost and complexity of operating manned aircraft.

The U.S. Department of Jutice, Bureau of Justice Statistics, published a report in 2007 that examined the use of aviation assets in law enforcement organizations with 100 officers or more. They identified 201 aviation units operating in 46 states. Those units spend more than $300 million in one year on aircraft purchases, leasing, financing, maintenance, and fuel, an average of $1.5 million per aviation unit. Although almost all law enforcement agencies would benefit from aviation units, few can afford them. UAS provide an affordable solution for specific support to tactical teams, forensics, fire safety, high-risk warrants, marijuana eradication, photographing critical infrastructure, corrections, traffic management for ingress/egress under special conditions, payload detection of HazMat (following train derailments), aid in evacuation after natural disasters (wildland fires, floods), critical incidents, and post-event forensics.

Recent Policy & Program Developments

Several constructive policy and program development actions are underway to advance UAS integration within the National Airspace System (NAS) and the public safety mission space.

National Airspace Integration

The FAA's principal concern about UAS operations in the NAS is safety. The NAS encompasses an average of more than 100,000 aviation operations per day, including air carrier, air taxi, general aviation, and military aircraft. There are approximately 18,000 air carrier aircraft and 230,000 active general aviation aircraft in the U.S. It is critical that UAS do not endanger current users of the NAS, including manned and other unmanned aircraft, or compromise the safety of persons or property on the ground.[3] The demand for airspace to test new systems and train UAS operators has quickly exceeded the current airspace available for military operations. DoD UAS operations conducted outside of restricted, warning, and prohibited areas are authorized only under a (temporary) Certificate of Waiver or Authorization (COA) from the FAA.

The COA authorizes an operator to use defined airspace and includes special provisions unique to the proposed operation. For instance, a COA may include a requirement to operate only under Visual Flight Rules (VFR) and/or only during daylight hours. Most COAs require coordination with an appropriate air traffic control facility and may require the UAS to have a transponder to operate in certain types of airspace. Due to the inability of UAS to comply with "see and avoid" rules as manned aircraft operations do, a visual observer or an accompanying "chase" aircraft

(Continued on Page 14)

[3] Federal Aviation Administration, Fact Sheet – Unmanned Aircraft Systems (UAS), Updated July 2011, Washington, D.C.

Combating Fatigue in Aviation Operations

by David A. Buczek, CIP/HS Fellow and President, DB&A*

Fatigue in aviation operations can present a hazard to the safety of the flying public and to aviation infrastructure. Recently, snoozing air traffic controllers and sleepy pilots overshooting their destinations have been in the headlines. Now, fatigue has become the focus of congressional hearings, new governmental regulations, and the media. But what exactly is fatigue, and what opportunities exist to manage the risks fatigue presents to the safety of aviation operations and the protection of aviation infrastructure?

Fatigue and Its Impacts

Fatigue can be defined as a physiological condition that reduces a person's ability to perform mental and/or physical tasks and increases the risk of injury or accident. Fatigue leaves workers feeling groggy, weary, and sleepy, and results from lack of adequate sleep or extended periods of wakefulness. It may also result from the time of day, such as an overnight shift, or from prolonged mental or physical activity.

Everyone experiences fatigue at some point each day; and that is normal. But, when aviation professionals are overly tired, fatigue can intrude on work life. Fatigue slows mental reaction times and causes people to make mistakes, even in well-practiced activities. Fatigued workers have difficulty concentrating, lose the ability to effectively anticipate events or actions, and lose the ability to communicate effectively with coworkers. Fatigue is unpredictable and causes variations in performance—one minute we feel alert, and the next we can find ourselves nodding off.

In safety-critical functions, fatigue poses a real hazard. Investigations by the National Transportation Safety Board (NTSB) into aviation accidents have shown numerous instances where fatigue was a contributory factor to the event, and one case where it was the primary cause of the accident that resulted in a hull loss and severe injuries to the flight crew.[1]

Fatigue can also cause serious health consequences. In most aviation operations maintenance work is often done at night, and flight and cabin crew work long and strenuous hours, often crossing timezones and dealing with "jet lag." Working at night when the human body craves sleep and attempting to sleep during the day when the body wants to be awake results in poor sleep and accumulating fatigue. Crew and maintenance personnel who work extended hours report increased

use of sick leave, more health complaints, and more doctor visits than workers in traditional daytime jobs. Sleep loss has also been associated with greater amounts of stress, alcohol and drug abuse, obesity, diabetes, and a lower sense of overall well-being.

When Is Fatigue a Hazard?

Research shows that being awake for 17 hours can impair neurobehavioral performance comparable to a blood alcohol level (BAL) of 0.05 percent. Being awake for 24 hours can impair performance to the equivalent of

(Continued on Page 7)

[1] Uncontrolled In-Flight Collision with Terrain AIA Flight 808, Douglas DC-8-61, N814CKU.S. NAS, Guantanamo Bay, Cuba, August 18, 1993, NTSB Report Number AAR-94-04, Dated 5/10/1994.

(Continued from Page 6)

0.1 percent BAL.[2] While most of us do not stay up for 24 hours very often, small amounts of sleep loss each day can build up over the course of a week and result in a highly fatigued condition. There are strict rules in aviation operations about working while under the influence of alcohol, yet the scheduling of some of our aviation operations may be placing our workers in a similarly compromised position.

According to recent studies,[3] humans are poor judges of their own fatigue. After being awake for long periods, our subjective feelings of fatigue remain low while our performance decrements increase.

When fatigue sneaks into our work life, we are ill-prepared to recognize or manage it. As a result, the FAA in its recent final ruling on pilot fatigue, instituted strict limits on work hours for Part 117 air carriers,[4] and the FAA has taken positive steps to address fatigue in air traffic control operations as well. All of this is an attempt to take our inability to recognize and address fatigue out of the safety equation.

Causes of Fatigue in Aviation Operations

The very nature and design of aviation operations can induce fatigue in workers. For flight and cabin crew, flying multiple segments (or flights) in a single day is taxing and can induce both mental and physical fatigue. Long flights, layovers, trying to rest in noisy accommodations, crossing timezones and attempting sleep when the local time is out of sync with the individual's body clock, can all impair recuperative rest leading to an accumulation of fatigue.

Mentally demanding work can quickly drain cognitive reserves. Experienced air traffic controllers, for example, who are handling a heavy traffic load are pushed mentally and experience "eustress," that feeling of "being in the zone" and performing at peak effectiveness. Inexperienced air traffic controllers, faced with the same heavy traffic load may experience "distress," a feeling of anxiety when trying to perform at the expected level of effectiveness. Both eustress or distress are mentally draining and can lead to fatigue.

In a similar but reverse function, monotonous or low-intensity work, especially at night, signals the brain to take advantage of downtime and seek rest. This can cause inattention or dozing off—what fatigue scientists call "microsleeps." Well-rested test subjects began to experience microsleeps after only eight minutes of straight-road

(Continued on Page 17)

[2] *Fatigue, Alcohol and Performance Impairment*, Dawson, et al., Nature, Vol. 388, July 17, 1997.
[3] *The Cumulative Cost of Additional Wakefulness,* Van Dongen, et al., SLEEP, Vol. 26, No. 2, 2003.
[4] *Flightcrew Member Duty and Rest Requirements*, Department of Transportation, Federal Aviation Administration, 14 CFR Parts 117, 119, and 121, Docket No.: FAA-2009-1093; Amdt. Nos. 117-1, 119-16, 121-357, RIN 2120–AJ58, December 21, 2011.

The Inactivation of the Body Scanners

by Michael Grabell, ProPublica*

X-raying passengers for airline security became a lot less common in 2012.

The use of radiation by security agencies, especially at airport checkpoints, was the subject of a ProPublica series in late 2011 and early 2012.

The investigation found that the Transportation Security Administration had glossed over the small cancer risk posed by even low doses of radiation. The stories also showed that the United States was almost alone in the world in X-raying passengers and that the Food and Drug Administration had gone against its own advisory panel, which recommended the agency set a federal safety standard for security X-rays. In addition, ProPublica reported that, outside airports, other security agencies are exposing people to radiation in more settings and in increasing doses.

Now, many of the TSA's 250 X-ray body scanners worth about $14 million are sitting in a Texas warehouse after being removed from most of the biggest U.S. airports, including Los Angeles, Chicago O'Hare, New York's John F. Kennedy, Boston Logan, Charlotte Douglas and Orlando.

The TSA said it replaced the X-ray machines with scanners that use another technology, millimeter waves, to make the lines move faster, allowing the agency to screen more passengers for explosives. But the result, intended or not, is that far fewer airline passengers are being exposed to radiation during screening. Millimeter waves, a form of high-frequency radio waves like those used in cell phones, have not been shown to cause cancer.

The manufacturer of the X-ray scanners, Rapiscan Systems, has also faced problems in developing its privacy software. Such software produces a generic cartoon image of passengers' bodies, allaying privacy groups' complaints that the scans amount to a "virtual strip search." The TSA faces a June 2013 congressional deadline to install the software on all its body scanners.

In November, the TSA sent Rapiscan a "show cause letter," which is typically issued when the government is considering terminating a contract. The agency hasn't said why. Rapiscan said the letter questioned whether the company changed the machine in a way that didn't conform with the design the TSA approved. Rapiscan says it did conform.

Rep. Mike Rogers, the Republican head of the House transportation security subcommittee, cited an alegation that Rapiscan had falsified a software test, which the company denies.

Following months of congressional pressure, in December, the TSA agreed to contract with the National Academy of Sciences to evaluate the health effects of body scanners. A provision to require such a test was included in the Homeland Security funding bill that passed the Senate appropriations committee in May; the final bill has not yet passed. It is not clear if the proposed study will add much to what is already known about the scanners, because it's unclear if the academy will conduct new tests of the machines or merely review previous studies.

Passengers traveling through Seattle-Tacoma, Phoenix Sky Harbor, Washington Dulles, and several other airports still must pass through an X-ray scan or opt out and receive a pat-down search.

The TSA says it hopes to eventually move the scanners from storage to smaller airports after resolving the issue with Rapiscan. In addition, the agency is considering an X-ray machine made by another company under a contract for the next generation of body scanners.

The last X-ray scanners in use in Europe were removed from

(Continued on Page 9)

(Continued from Page 8)

Manchester Airport in the United Kingdom in September. Israel, which is small but influential in the security world, has installed an X-ray body scanner for testing at Ben Gurion Airport in Tel Aviv.

A side-by-side comparison of the TSA's body scanners, including photographs of them, can be found here. And here are some key points about the two types of scanners:

Safety: The X-ray machine, known as the backscatter, uses ionizing radiation, which has long been linked to cancer. According to many studies, the dose of the machine is very small, equivalent to the cosmic radiation received in a few minutes of the flight. The TSA cites those studies in claiming they're safe. The National Academy of Sciences has concluded that there is no known dose of radiation that does not increase the risk of cancer, and radiation groups recommend that the public limit its exposure as much as reasonably possible.

Although there has been some doubt about the long-term safety of millimeter waves, scientists have not found a mechanism for such waves to mutate genes and cause cancer.

Privacy: The millimeter wave machine contains privacy software that scans a passenger's body for anything unusual that might be hidden under his or her clothes. It then creates a generic image of a body and highlights any potential threat with a yellow box. No human being analyzes the image; it is all automated.

The manufacturers of the X-ray scanner are working on similar software. But for now, the machine creates a heavily filtered image of the person's naked body, which is viewed in a separate room by a TSA screener who cannot see the passenger.

Detection: Federal officials have released no information about the detection rates of the two machines. Security experts say that in their original forms, the image of the X-ray machine was clearer than that of the millimeter wave machine. But any difference was made minimal through training and now by the computer algorithms that automatically scan the passenger, they say. Government inspectors have repeatedly found "vulnerabilities" with the machines, but to what degree is not known.

False alarms: Based on reports and interviews with foreign officials, the millimeter wave machine has a much higher false-alarm rate than the X-ray scanner, tripping on innocuous things such as folds in clothing, ties and even sweat. Those false alarms require a quick search of the area where the anomaly was detected, whereas alarms with the X-ray scanner usually require a full-body pat-down. ❖

*This article was originally published by ProPublica and can be found at http://www.propublica.org/article/the-inactivation-of-the-body-scanners.

LEGAL INSIGHTS

Grant-Free Airport Infrastructure Project Funding - The Time Has Arrived

by Gregory Walden, Adjunct Professor of Law
George Mason University School of Law*

You might be surprised to learn that Congress can ensure a healthy and reliable source of airport infrastructure funding without appropriating a single dollar, and indeed in doing so may reduce Federal spending by billions of dollars. Before showing how this feat is possible, it helps to provide the legal and historical contexts of Federal funding for airport capital projects.

Since 1946 the Federal Government has funded the birth and development of commercial service airports. The current Airport Improvement Program (AIP) was established in 1982 and has been extended with each subsequent reauthorization of Federal Aviation Programs. Under current law, Federal grants generally pay 75% of the costs of large airport eligible projects, and 90-95% of the costs of small airport eligible projects. But Federal funding is not the only or even primary source of funding for many airport capital projects. Airports have also funded capital projects through bonds (the revenue from rates charged to airlines, concessionaires, and other airport tenants and users is generally spent on operating costs).

Since 1990, airports have been authorized by Congress to impose and use a Passenger Facility Charge (PFC) on each paying departing passenger, subject to FAA review and approval. (Congressional authorization was necessary because the Anti-Head Tax Act of 1973 prohibits local governments from charging a passenger fee.) The PFC initially was limited to $3.00 and raised to $4.50 (requiring additional justification) in 2000. The ability of larger airports to tap into PFC revenue has allowed the FAA substantial leeway to fund small airport projects under the AIP program, although larger airports also regularly rely on AIP funding for projects that are relatively modest in scope, and occasionally rely on much greater AIP funding under a multi-year Letter of Intent to pay for a new airport, new runway, or taxiway.

Airports in this country may appear to be in much better shape than roads and bridges, but runways, like roads, must also be repaired and repaved from time to time. Also, safety requirements imposed by the FAA require a significant investment. AIP funding, which has in recent years been authorized at a level between $3.25 and $4 billion per year, has been adequate to cover these maintenance and safety requirements. It is larger projects, such as building a runway or taxiway, where airports have turned to the PFC revenue stream to pay for these projects directly, or to pledge PFC revenue to pay back airport bonds.

As aviation is expected to grow substantially over the next decade, commercial service airports, especially international airports, will need to expand both airfield and terminal capacity. At the same time, it is uncertain whether Congress will continue to appropriate AIP funding at the same levels as it has in the past. AIP grant funds, derived from the Airport and Airway Trust Fund, are exempt from sequestration. However, AIP funding is not protected against a reduction in appropriated funds. Moreover, the Trust Fund (like the Highway Trust Fund, albeit for different reasons) is in a squeeze. As airlines unbundle fares, removing so-called ancillary fees (for food and checked bags) from the ticket price, this revenue is not subject to the 7.5% ticket tax, which is the largest source of Trust Fund revenue. And the Trust Fund also pays for a portion of the FAA Operations Account.

The American Recovery and Reinvestment Act (ARRA) of 2009, popularly called the Stimulus Bill,

(Continued on Page 11)

(Continued from Page 10)

bestowed two funding benefits to local governments. The Build America Bonds program provided for Federal subsidies for a portion of the interest costs, and an exemption from the Alternative Minimum Tax treatment of interest generated by airport private activity bonds, significantly spurred airport financing, in addition to a one-time infusion of Federal grants for shovel-ready airport projects apart from the annual AIP appropriation. This robust Federal support for airport infrastructure projects from 2009 to 2011 masked the problematic state of airport funding. When these programs expired, and Congress then enacted an FAA reauthorization bill with no PFC increase and with a modest reduction in AIP authorized funding, the true state of airport funding came into focus.

Fortunately, the way to ensure adequate funding for large airport capital projects that are needed now or will be in the future does not require Congress to increase Federal spending. Indeed, the FAA budget, which includes AIP grants, can be reduced by $400 million or more each year. This can be accomplished simply by removing the statutory cap on the PFC for the 29 large hub airports, and making such airports no longer eligible for Federal airport grants (excepting continuing payments under existing Letters of Intent). The Obama Administration budget proposal recommends both large and medium hub airports (65 in total) be removed from the grant program. And the list of illustrative savings accompanying the Simpson-Bowles report also recommended that large and medium hub airports no longer receive AIP funding. Both proposals estimate the annual Federal budget savings to be from $1.1 to $1.2 billion. Both proposals assume that larger airports can take care of themselves through passenger fees: the Obama Administration recommends the maximum PFC be increased to $7.00; Simpson-Bowles does not recommend any increase. But this assumption is flawed. These proposals do not take into account that all of the $4.50 PFC-based revenues at most large hub airports are committed over the next 10 to 20 years to pay for projects directly or to pay debt service. Also, the purchasing power of a $7.00 PFC in 2013 does not even equal the value a $4.50 PFC had in 2000. These proposals work only if the airports that are no longer eligible for AIP grants are allowed to raise the PFC as necessary for airfield and terminal capital projects, without any artificial limit.

Allowing large hub airports the freedom to set a PFC will reduce the pressure on the Airport Improvement Program while allowing smaller airports to obtain AIP funds without competing with the greater demands of large hub airports. The large hub airport with the least enplanements (a little over 8 million) can cover the amount it generally receives in AIP grants by raising its PFC only two dollars or so. Some of the largest airports can fund the entire cost of a new runway through a two dollar PFC increase over a period of years. For many medium hub airports, however, foregoing AIP grants might require a PFC increase of five to ten dollars or more to cover the cost of a major capital project. Even so, the increase in the PFC will be far less than the fee most airlines charge for a single checked bag. Devolution of large airport funding is sound public policy, either from the standpoint of vesting control of airport growth in the local government that owns and operates that airport, or as an acknowledgment of and a contribution to the deficit reduction imperative Congress faces.

There is much cross-subsidization in the current AIP program, largely benefitting smaller airports. A PFC involves no cross-subsidy; the PFC revenues generated at an airport are retained by the air carrier in escrow to be used only for projects at that airport (or another airport under the same ownership). Large hub airports can indeed fend for themselves, but only if allowed to impose a PFC in an amount necessary to pay for a capital project, either directly or as payment of bond debt. Compared with ensuring adequate funding for highways, transit, or bridges, the task for Congress to ensure adequate funding for large airports is quite simple: remove the PFC cap, and pocket billions of dollars in Federal savings. ❖

*The author is also of counsel with Patton Boggs LLP, where he practices aviation law. The opinions expressed in this article are those of the author and do not necessarily reflect the views of the author's firm or clients.

(Continued from Page 3)

vulnerabilities that could provide an attacker with immediate access into a computer system and allow remote execution of commands.[6] A follow up report indicated that while FAA has taken steps to install some advanced systems in ATC facilities to detect cyber threats, most sites have still not been upgraded. In addition, a U.S. General Accounting Office (GAO) report lists several incidents where satellite services have been disrupted or denied as a result of system vulnerabilities. The DoD and GAO cite several types of threats to critical satellite-based systems including ground-based, space-based, and interference-oriented threats.[7] FAA operational requirements necessitate the use of *unencrypted* ADS-B data links, which the agency believes have a low likelihood of malicious exploitation.[8]

However, research conducted by the United States Air Force's Institute of Technology concluded that ADS-B's unencrypted signals are susceptible to interception, jamming, and spoofing that could result in loss of situation awareness, service disruption, and potentially crashes.[9] A recent report on Global Navigation Satellite System (GNSS) jamming discusses the susceptibility of the signals to radio frequency interference (RFI) due to: a) *malicious interference,* b) *uninformed interference* (i.e., intentional transmission of signals without intent to cause harm), and c) *accidental interference* from unintentional signal transmissions.[10] Most occurrences have involved uninformed and accidental interference. This report cites recent incidents at Newark Airport and a Leesburg, Virginia site where truck drivers using personal privacy devices (PPDs) to block position tracking by employers have caused unintentional interference with signals from both ground-based and space based GPS augmentation systems.[11] In a more publicized incident, the FCC denied Light Squared's venture to deploy an expanded wireless broadband network because it used adjacent radio spectrum that increased the proability for unintended interference with the Global Positioning System (GPS) signals.[12]

These examples highlight the intersections between the objectives of government and industry stakeholders, and between public and private users of cyber infrastructure. While these cases illustrate the potential threats and challenges, they also represent opportunities to resolve these vulnerabilities and improve the overall resilience of our air transportation infrastructure. The evolution of policies, procedures, certifications, and standards often lags technology development and implementation, but are essential to resolve conflicting interests and concomitant vulnerabilities. Finally, these instances underscore the need to address the vulnerabilities of: a) the physical sources of information (e.g., satellites, systems, sensors), and b) the cyber infrastructure (e.g., data links, information systems, network and processing mechanisms, cloud-based applications) that represent the NAS enterprise architecture.

Seven Steps Toward Improved Risk Management and Resilience

1. **Recognize that it takes a network to defend a network.** Protecting a system-of systems such as our air transportation infrastructure involves far more than having

(Continued on Page 13)

---

[6] U.S. Department of Transportation. 2009. "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems." Federal Aviation Administration. Report Number: FI-2009-049. May 4, 2009.

[7] United States General Accounting Office (GAO). "Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed," Report #: GAO-02-781. August 2002.

[8] McCallie, Donald; Butts, Jonathan; Mills, Robert. 2011. "Security Analysis of ADS-B Implementation in the Next Generation Air Transportation System." *International Journal of Critical Infrastructure Protection*. Volume 4, Issue 2, pp 78-87. Elsevier, August 2011.

[9] Ibid.

[10] Pullen, Sam, and Grace Xingxin. 2012. "GNSS Jamming in the Name of Privacy: Potential Threat to GPS Aviation." *Inside GNSS.* March/April 2012: 34-43.

[11] Ibid.

[12] Davis, Dee Ann. 2012. "Light Squared Fallout May Drive Push for GPS Receiver Standards." *Inside GNSS.* March/April 2012: 20-26.

(Continued from Page 12)

the right technology. It also involves people, policies, and analytics to proactively detect threats and counter them before consequential events occur.

2. **Develop a Cyber Security Enterprise Architecture** (Cyber EA) as an integral layer of the NAS enterprise architecture. Building in protection and resiliency at the enterprise level (versus just at the individual system level) is imperative if we are to effectively and economically thwart threats to aviation safety and security. The Cyber EA must include provisions for certifications, policies and standards, and appropriate enforcement mechanisms such as authentication, inspection, classmarks, and proxies. The Cyber EA would establish the blueprint for a scalable, enterprise-level security framework. This framework would enable future capabilities to be implemented that employ enterprise security controls, not just isolated system-specific provisions. We must move beyond "check-the-box" compliance to flexible models that adjust to the changing technological and operational environments.

3. **Improve systems integration testing** to ensure that the incremental evolution of the NextGen system-of-systems remains secure as new capabilities are introduced. The increased use of open systems architectures, COTS products and equipment, etc. may inadvertently introduce new vulnerabilities. Security requirements and specifications can be developed for customized vendor products and solutions. However, it is only through *enterprise systems integration testing* and independent verification and validation (IV&V) that emergent vulnerabilities can be identified and resolved prior to operational deployment.

4. **Establish a unity-of-effort to implement a dynamic defense posture.** Evolving threats can change on a daily and even hourly basis. The FAA and other government and industry stakeholders can create cyber resilience by recognizing that cyber security is not just about technology, but also about people—because they are so critical to an organization's ability to protect itself. Considering the diverse stakeholders and objectives at play, we need a unity-of-effort to develop effective policies, standards, certifications, and engineering solutions that are acceptable by public and private stakeholders with divergent objectives.

5. **Create cyber resilience in addition to cyber defenses.** Cyber resilience is the ability to operate in the face of persistent attacks. Traditional cyber defense strategies, such as firewalls and intrusion-detection systems, are no longer enough. Cyber attacks on our critical infrastructures—including our air transportation system—are becoming so numerous and sophisticated that some inevitably get through. Resilience enables the FAA Air Traffic Organization to continue to provide service to the public and industry customers while fending off or reacting to cyber attacks.

6. **Develop and deploy sophisticated cyber analytic tools** to connect the dots across the massive amounts of flight data, CNS information, and mission support data. The network-centric ATC systems architecture creates an opportunity to apply "cloud analytics" to process dynamic data from distributed sources and identify the trends, anomalies, and relationships that lead to proactive threat detection.

7. **Implement advanced Cyber Training to educate the next generation of cyber professionals** on the latest tools, tactics, and techniques, so that they can implement solutions that meet future cyber threats and challenges head-on. Effective cyber training requires a *holistic approach* that involves people, processes, and technology. Threats are dynamic and evolving. Therefore, cyber training must be an integral part of an organization's continuous improvement process rather than just a one-time exercise to earn a certificate, accreditation, or other recognition. ❖

(Continued from Page 5)

must maintain visual contact with the UAS and serve as its "eyes" when operating outside of airspace that is restricted from other users.

Because of their inherent differences from manned aircraft, such as the pilot removed from the aircraft and the need for "sense and avoid," introduction of UAS into the NAS is challenging for both the FAA and aviation community. In addition, UAS must be integrated into an evolving NAS, as the airspace management infrastructure transitions from one that is today based upon ground-based navigational aids to a future GPS-based system in FAA's NextGen. Recognizing that new UAS standards and guidance is a long-term effort, and to address the increasing civil market and the desire by civilian operators to fly UAS, the FAA is developing new policies, procedures, and approval processes. These include:

- Creation of the Unmanned Aircraft Program Office to integrate UAS safely and efficiently into the NAS.

- Establishment of the UAS Aviation Rulemaking Committee to bring inputs and recommendations to the FAA on UAS matters.

- Tasking the RTCA[4] —a group that has advised the agency on technical issues for over 77 years—to work with industry and develop UAS standards as to how to handle UAS communication, command, and control, and how to "sense and avoid" other aircraft.

FAA UAS Test Sites

The FAA Modernization and Reform Act of 2012, signed into law by the President on February 14, 2012, includes specific requirements for UAS and national airspace. Under H.R. 658, Section 331(c), the FAA Administrator is required to establish a program to integrate unmanned aircraft systems into the national airspace system at six test ranges. Per 14 CFR Part 91 [Docket No. FAA-2012-0252] the FAA engaged the matter of Unmanned Aircraft System Test Sites through a "Request for Comments" action in the Federal Register.[5] The FAA intends to identify six test ranges/sites to integrate UAS into the NAS some time in FY 2013. The FAA believes that designation of such UAS test sites will assist in the effort to safely and efficiently integrate UAS into the NAS.

Sensors

As complex as UAS platform selection and pilot training is, the challenge of selecting, acquiring, and managing a wide range of sensors to exploit the UAS for a multiplicity of operational mission needs may be as daunting. Remote sensing functions include electromagnetic spectrum sensors, gamma ray sensors, biological sensors, and chemical sensors. Electro optical (EO) or electromagnetic sensors typically include visual spectrum, infrared, or near infrared cameras as well as synthetic aperture radar or other radar systems. Other detectors such as microwave and ultraviolet spectrum sensors may also be used. Biological sensors are sensors capable of detecting the airborne presence of various microorganisms and other biological factors. Chemical sensors typically use laser spectroscopy to analyze the concentrations of each element in the air. Radiological sensors are used for radiation background baselining to facilitate emergency searches for suspected nuclear or radiological materials. Acoustic sensors have a valuable role in identifying humans in both search and rescue and border protection settings. RF sensors can be effectively used to detect radio equipment or cell phones in use in restricted areas near perimeter of sensitive facilities or in border or other high-risk areas. Sensor systems require operators who are trained on their proper use and their skill sets are and will remain in high demand.

(Continued on Page 15)

[4] RTCA was founded in 1935 as the Radio Technical Commission for Aeronautics; September 30, 2012; www.rtca.org.

[5] U.S. Government Printing Office (GPO), Federal Register, 14 CFR Part 91 [Docket No. FAA-2012-0252], Washington, D.C.

(Continued from page 14)

Communications, Interoperability, and Security

Successful integration of UAS into a public safety agency's infrastructure will necessarily address elements of system command and control, sensor data acquisition, data security, handling, and retention. Attributes that must be addressed include (a) sense and avoid: traffic alert and collision avoidance; (b) management of a lost link and the uncontrolled landing contingency; and (c) an interoperable communications architecture. Each of these dimensions of system integration and lifecycle management brings with it a long tail of policy development or revision; creation of new operational procedures; updates to plans, and enhancement of training and exercises; quality assurance surveillance to maintain standards of privacy, data security, and operational security; and, the fundamental logistics and maintenance program sustainment requirements.

As with public safety communications, "interoperability" is the keyword. To be technically interoperable, standard digital communications techniques linking the UAV pilot to aircraft controls (including video and sensors as well as weapons systems) and the aircraft ISR data to ground observers and decision-makers has been developed. The interoperability goal for unmanned systems is an ability to provide data, information, material, and services to and accept the same from other systems, units, or forces … and to use the exchanged data, information, material, and services to enable them to operate effectively together.

The FAA's UAS Integration Office in collaboration with the National Institute of Justice (NIJ) has designed a solution that would permit the operation of small UAS (SUAS) in a less restrictive manner than current FAA policy. While the COA process will continue, many of its barriers will be reduced through streamlined on-line applications. The FAA plans to develop a master list of SUAS that an agency can use to select the aircraft with appropriate equipment. Manufacturers will be able to have their aircraft included in this master list through an independent assessment process, as yet undefined. It is anticipated that with model standard operating procedures, operating limitations and training curriculum, agencies will have a simplified and timely process in applying for COAs.

Cybersecurity challenges to assure UAS operations include spoofing, denial of service attacks, hacking and hijacking. Vulnerabilities with the Global Positioning System (GPS) can be exploited by an enemy and used to "hijack" a drone. In a test sponsored by the DHS, a team from the University of Texas at Austin successfully "spoofed" a drone with equipment worth only $1,000 – feeding false information to its GPS in an effort to bring it down. Solutions must prove resistant to spoofing and other forms of cyber-attack. The cybersecurity of UAS operations must be considered in lockstep with the overarching NextGen NAS cybersecurity planning and vulnerability assessments.

Privacy, Data Retention and the Role of Fusion Centers

The subject of privacy and data security associated with UAS surveillance and monitoring data products cannot be adequately treated in this forum. UAS technology is now making its way into the hands of law enforcement, fire, hazmat and other emergency response professionals nationwide.[6] Personal rights are cherished and legally protected by the Constitution. Concerns about privacy rights could threaten the full realization of the benefits of this technology in the public safety mission. The International Association of the Chiefs of Police (IACP) Aviation Committee has been involved in the development of unmanned aircraft policy and regulations for several years and has demonstrated thoughtful leadership on these sensitive issues by recently publishing recommended guidelines for agencies contemplating the use of UAS.[7] Related to privacy considerations, the American Civil Liberties Union recently published

(Continued on Page 16)

[6] Rogers, Keith, "Agency Working on Code for Drones Amid Privacy Concerns," *Las Vegas Review-Journal*, Las Vegas, Nevada, August, 31, 2012; http://www.lvrj.com/news/law-enforcement-use-of-unmanned-aerial-vehicles-raises-privacy-concerns-168222656.html.

[7] IACP, *Recommended Guidelines for the Use of Unmanned Aircraft*, Aviation Committee, p. 3, Washington, DC, August 2012.

(Continued from Page 15)

a set of recommendations regarding use of "drones." On February 24, 2012, the Electronic Privacy Information Center, joined by over 100 organizations, experts, and members of the public, submitted a petition to the FAA requesting a public rulemaking on the privacy impact of drone use in U.S. airspace.[8]

Management of UAS data streams will benefit from careful analysis of lessons learned from the implementation of privacy policy guidelines and best practices instituted by our Nation's intelligence fusion centers. The role of the fusion centers in regional sharing of UAS resources and particularly in managing new data streams from UAS assets must be pursued, as the benefits of UAS are not restricted to preparedness and disaster response under the auspices of a singular jurisdiction or even a regional emergency management entity. Nor is it limited to fire or hazmat response functions managed from an EOC or Incident Command Post. Indeed, UAS platforms offer real time surveillance, investigations, and law enforcement tactical response capabilities and therefore data derived from these systems must be treated as law enforcement sensitive information of potential evidentiary value to prosecution of criminal activities. That fact will drive collection and retention guidelines. Because state and local statutes regarding the retention of data, e.g., video surveillance data, vary widely across the Nation, the data management model for effective and legal use of UAS collection capabilities requires careful, tailored planning in each regional setting. Approaches to these policies reinforce (a) the value of the fusion center model as a coordination framework for integration of new UAS-based information resources with deep experience in privacy policies and protection; and, (b) the importance of current and comprehensive operational plans for sharing these capabilities within a UASI region or through other interagency partnerships.

Over the Horizon

There are numerous issues associated with UAS integration within the public safety domain that demand further research. Work remains to enhance understanding and enable adequate plans, policies, and best practices for effective integration of these beneficial assets into the civilian airspace. Within Nevada the successful use of UAS for overflight of dams and levees at risk proved invaluable during recent flood events.[9] Building on that experience and others and in conjunction with the development of a response to the FAA UAS Test Site solicitation, a consortium of industry and university partners are working with the public safety community in southern Nevada to develop a roadmap for future technical assistance and training. Drawing from lessons learned with the DHS technical assistance programs supporting the homeland security enterprise, *The Roadmap for a Public Safety UAS Technical Assistance Program* will address planning considerations and sustainment needs for public safety UAS programs ranging from requirements definition and acquisition strategies to sensor package selection and integration; actions to assure data handling and communications comprehensively address security, privacy protections, and education to assure public trust; and, planning, training, and exercises to assure successful integration within the interlocking, intergovernmental emergency response framework.[10] The *Roadmap* is one of many educational resources we will need to effectively integrate the UAS technologies into the civilian NAS in service to our public safety. ❖

* Robert J. Coullahan, CEM, CPP, is the President of Readiness Resource Group Incorporated (RRG) in Las Vegas, Nevada; coullahan@readinessresource.net.

* Robert I. Desourdis, Jr. is the author of multiple books on communications design and engineering and public safety interoperability and is based in Fairfax, Virginia; achieving_interoperability@yahoo.com.

[8] *See* http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.
[9] Mr. Steve Endacott, Director of Emergency Management, Fallon, Nevada in a presentation on December 5, 2012, Las Vegas, NV.
[10] Robert J. Coullahan, Readiness Resource Group, is leading this Roadmap development activity.

(Continued from Page 7)

driving in a simulator.[5] Without stimulation, we all can experience fatigue-like symptoms in a short period of time.

For maintenance workers shift work can cause fatigue as well. Normally, people are wired to be awake during the day and asleep at night. Sometimes referred to as our "internal body clock," exposure to sunlight kicks our body into gear in the morning, and darkness initiates our sleep system in the late evening. When scheduled to work a midnight shift, we work against our body clock, and our sleep/wake patterns are disrupted. When we try to catch up on sleep during the day, our body wants to be awake, and our sleep is not as long, deep or restorative. If we do not get the eight hours of necessary sleep each day, fatigue builds over time; this is called sleep debt. By the end of a work week, we can be dangerously fatigued. Adequate rest or nap breaks (if possible) on midnight shifts help trim our sleep debt and keep us alert while working nights.

Even when employers offer fatigue-friendly shift patterns, balance mental demands of the job, and offer adequate rest breaks, if employees do not properly manage their own sleep hygiene, fatigue can still find its way into the workplace. When employers provide rest opportunities between work shifts, employees need to take advantage of them. Employees should be well-educated about fatigue and its associated health and safety risks, countermeasures they can employ to manage fatigue in their personal lives, and ways to protect their sleep each day.

Mitigating Fatigue in Aviation Operations

The first step in mitigating fatigue in aviation operations is identifying where it might be present. Biomathematical fatigue models are software-based tools that are used to assess levels of fatigue in workers as they progress through work shift patterns. Sophisticated algorithms in these tools take into account the human body's sleep/wake rhythms, the need for sleep, and the decremented performance caused by hours of wakefulness. The modeled results allow aviation safety professionals to identify shift patterns or city pairs that increase fatigue hazards and generate "what-if" alternatives that may reduce those hazards.

Aviation safety staff can also analyze existing data sources to identify associations or patterns between possible fatigue hazards and specific workplace events or incidents. Data from Flight Operation Quality Assurance (FOQA), Aviation Safety Action Program (ASAP), and more specifically, FAA-required fatigue reporting systems can be analyzed to define specific causal or contributory factors that lead to fatigue.

In risk analysis, the aviation safety professional can utilize modeling and safety-related data analysis results to identify how often a fatigue hazard is present and the time of day it occurs. The severity of a fatigue hazard, represented as decremented cognitive performance, then needs to be defined. Bringing together operational Subject Matter Experts (SMEs) with knowledge of risk areas and operations is necessary to assess when fatigue can be accepted and when it establishes a risk that must be mitigated.

With knowledge of exposure data, hazard and risk analysis results, and an understanding of the unique aviation operations environment where a fatigue risk exists, mitigations that are specific to each risk can be engineered. By addressing each risk individually—preventing fatigue from occurring or controlling it once it is present—fatigue risk can be controlled to acceptable levels and the safety of aviation operations maintained.

The Impact on Aviation Infrastructure

Flight and cabin crew need to be alert and perform at their best to ensure the safety of the customers in their direct care. Maintenance staff likewise can have a direct impact on the flying public if fatigue-related errors creep into their work. Air traffic control personnel must also remain alert and vigilant while directing traffic and maintaining safe separation distances between aircraft. If staff in any of these roles allows fatigue-related errors to intrude on their work, the results could be catastrophic.

Aviation technicians who install and maintain the air navigation equipment used throughout the National

(Continued on Page 18)

[5] *An Examination of Monotony and Hypovigilance , Independent of Fatigue, a Relevance to Road Safety*, Rebecca Michael, PhD Thesis, 2011, Queensland University of Technology, Centre for Accident Research and Road Safety.

(Continued from Page 17)

Airspace System could potentially have an even bigger impact if errors intrude on their work. Landing systems could go offline, removing an airport from service, or air navigation radars could go offline, interfering with the availability of entire sectors of the national airspace. If fatigue is not managed in aviation operations it can lead to catastrophic events that disrupt the Nation's aviation infrastructure.

Many of today's 24/7 work environments are fraught with fatigue and aviation is one of them. NASA, for example, assumes fatigue to be present in its flight operations (both in-flight and ground control) and seeks to actively mitigate the risks that fatigue presents to the safe completion of a mission. All aviation safety professionals need to be aware of fatigue, its causes and impacts, and take active measures to identify, analyze and mitigate its effects on safe aviation operations. Doing so will avert potential aviation catastrophes and ensure the ongoing availability of aviation infrastructure. ❖

*David A. Buczek, MA, is the President of DB&A and is a Fellow at the George Mason University, Center for Infrastructure Protection and Homeland Security. He can be reached at (703) 861-5332 or dave.buczek@dbainnovation.com.

The Center for Infrastructure Protection and Homeland Security Presents:
Fatigue Risk Management in Aviation Operations

This Symposium will equip attendees with the knowledge and approaches necessary to effectivelty fight fatigue in the operational setting. The human physiology of fatigue and the hazards it represents in the workplace will be explored, along with the effective methods and tools to conduct fatigue risk management, mitigate fatigue's negative effects, and enhance public safety.

This one day session will be held January 31, 2013.

For more information on registration and program agenda, click here.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) 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).