

SPRING 2002

AWAKENINGS

911

*IASA and the GAO.
Did FAA take Security Seriously Prior to Sept 11?
The Transportation & Security Act 2002.
Bogus Aircraft Parts.
The Canadian Aeronautics Act.*

THE QUARTERLY MAGAZINE OF THE

INTERNATIONAL AVIATION SAFETY ASSOCIATION®

WWW.IASA-INTL.COM

Page 1

©2002 IASA International Aviation Safety Association. All rights reserved.
®International Aviation Safety Association and the IASA logo are registered trademarks of the
International Aviation Safety Association.

Spring 2002

AWAKENINGS

The Quarterly Magazine of the
International Aviation Safety Association

CONTENTS

No More Excuses	3-5
After concluding a series of meetings in both the U.S. and Canada, including the General Accounting Office, IASA looks at aviation safety post September 11.	
Past Present & Future	6-10
We strip away the rhetoric and examine the FAA's commitment to security prior to September 11.	
Will it ever be the same?	11-16
Jim Bennett takes an in-depth look at the Aviation Transportation and Security Act of 2001.	
Third International Aviation Security Symposium	17-18
Like a Curate's Egg, Good in Parts	19-26
John Sampson examines the trade in bogus aircraft parts and asks whether enough is being done to halt this illegal and potentially fatal activity.	
Aviation Security in Canada	27-28
Charlene Frenette assesses the impact of the Canadian Aeronautics Act - does this solely serve to diminish accountability?	
About IASA	29



No More Excuses

"Face to face" was IASA's strategy for a series of meetings that started in September 2001, and culminated in a meeting with the United States General Accounting Office in Washington D.C. on February 25th, 2002.

Has the aviation safety landscape changed post September 11?

In the months following the terrorist atrocities of September 11, IASA has repeated its calls for a fundamental rethink of how we regulate the aviation and related industries:

"Action not Reaction" said IASA Chairman Lyn Romano "September 11 could have and should have been avoided. As with Swissair 111 and too many others, we have to look at the regulatory framework that allowed more innocent people to be killed"

So how, if at all, has the aviation safety agenda changed since September 11? Is security the priority to the exclusion of all others?

"It is my belief that people are taking a long hard look at the obvious failings in regulatory oversight and seeing this as a generic problem within our system" continued Lyn "For years, I have been giving these agencies their own data and asking them why they either delayed taking action or didn't take any action at all."

Since September 2001, IASA has met with the **Federal Aviation Administration** (FAA), the **Transportation Safety Board of Canada** (TSB), **Transport Canada** (TC) and the **US General Accounting Office** (GAO).

"I have made it clear to everyone since Swissair 111 and again now as a result of September 11 – No More Excuses. If we are to ever effectively oversee air travel then we need to focus on what we can do as opposed to dwelling on what we cannot, and we need a regulator that will take an active role in promoting safety."

So what has been the outcome of IASA's latest round of meetings?

"Now that IASA has secured a permanent office in Canada and broadened the mandate of IASA Europe under new leadership, it was important that I saw for myself how effective IASA could be globally post September 11"

"I am pleased to say that any fears I had that security would dominate all discussions, to the exclusion of all other issues, were misplaced - at least as far as my meetings in Canada and with the GAO were concerned"

Below are details of IASA's recent meetings:

**FAA
September 27, 2001**

IASA Chairman Lyn S Romano met with *outgoing* Assistant Administrator, Tom McSweeney. The main topic of discussion was the TSB's August 28 recommendations titled *Material Flammability Standards*:

"I was shocked when I was informed that he [McSweeney] had not seen them," explains Lyn "In my opinion these recommendations represent one of the single most important series of findings and recommendations about aircraft wiring. To my knowledge, the FAA have still not made their response to them public and I am very disturbed at this"

TSB January 17, 2002

IASA Chairman Lyn S Romano met with Vic Gerden and Jim Harris in Ottawa.

"The TSB through their investigation into the crash of Swissair 111 are in

many respects leading the way in terms of recommendations concerning aircraft wiring and material flammability" said Lyn "Their wider role is secured by their objectivity and the expertise they have demonstrated to date"

**Transport Canada
January 17, 2002**

IASA Chairman Lyn S Romano and IASA Canada CEO, Charlene Frenette, met with senior representatives of Transport Canada – the Canadian equivalent of the FAA.

Also present was Safety Services staff members Jim McMenemy, Human Performance Specialist and George Leblanc, Technical Inspector, Continuing Airworthiness, among others.

The meeting was arranged as an introduction of IASA representatives to Transport Canada staff and included issues of aging aircraft wiring, the increase in runway incursions in Canada and CADORS, the Transport Canada Occurrence Reporting System.

**General Accounting Office
February 25, 2002**

On January 25, 2002, the GAO released a report titled "FAA and DOD Response to Similar Safety Concerns" [GAO-02-77] that examined, on a case-study basis, among other things, the FAA's response to concerns about aircraft wiring. The GAO is a stalwart, objective and, sometimes, critical observer of the FAA as demonstrated in other reports, however, this most recent report echoed many of IASA's concerns.

IASA Chairman, Lyn S Romano, and IASA (Europe) Chairman, Adam Smyth, had the pleasure of meeting:

- **Gerald L Dillingham PhD** (Director, Civil Aviation Issues)
- **Robert E White** (Assistant Director, Physical Infrastructure Team)
- **Bonnie A Beckett PhD** (Assistant Director, Aviation Issues)
- **Beverly N Dulaney** (Senior Analyst, Physical Infrastructure Team)
- **Anthony Patterson** (Analyst, Physical Infrastructure Team).

"It was such a wonderful opportunity for IASA to meet with the GAO and discuss issues of mutual interest," explained Lyn "I did not have the opportunity to meet with the GAO when they were represented at IASA's Symposium in November 2000 and so it was a real pleasure to meet with them in D.C."

"I have every confidence that IASA can look forward to a productive long-term working relationship with the GAO in promoting aviation safety issues of mutual concern"

"It was the first time since IASA's formation on March 4, 1999 that IASA USA and IASA Europe were both represented at such a high-level meeting in the US" continued Lyn "It was a fitting tribute to the new strides IASA has taken since we restructured over the past year or so and solidifies our commitment to tackling aviation safety issues on a global scale."



THE MEETINGS

September 27, 2001
Federal Aviation
Administration, D.C.
IASA USA Chairman

January 17, 2002
Transportation Safety
Board of Canada,
Ottawa
IASA USA Chairman

January 17, 2002
Transport Canada,
Ottawa
IASA USA Chairman
IASA Canada CEO

February 25, 2002
United States General
Accounting Office, D.C.
IASA USA Chairman

Past Present & Future

We look behind the rhetoric and examine the FAA's security record prior to September 11. Did the FAA help or hinder security?

By

ADAM SMYTH

Adam serves as Director of Legal & Public Relations on behalf of IASA USA and as Chairman of IASA (Europe).

You can contact him by email at:

adam.smyth@virgin.net

THE ATROCITY

At 8.48 am Eastern Daylight Time American Airlines Flight 11 crashed into the north tower of the World Trade Center. Fifteen minutes later the World watched as United Airlines Flight 75 crashed into the south tower. Thirty-seven minutes later American Airlines Flight 77 crashed into the Pentagon and twenty-three minutes later United Airlines Flight 93 crashed 80 miles southeast of Pittsburgh. Two minutes later the south tower of the World Trade Centre collapsed. Twenty-four minutes after that the north tower collapsed.

Within the course of one hour and forty-one minutes, the world as we knew it had changed forever.

THE SPIN

Security was the new priority at our airports and in our aircraft. Secretary of Transportation, Norman Mineta, spoke of 'more stringent levels of security' and 'heightened security measures'. Two Rapid Response Teams were convened, one to focus on increasing security at airports, the other on aircraft security, focusing on cockpit access.

Joint teams comprised of officials from the Federal Aviation Administration (FAA) and the Office of the Inspector General began auditing background checks of Argenbright Security Inc employees at 13 U.S. airports because of background check violations uncovered by the FAA.

New employees were hired to provide oversight and support at screening checkpoints, to assist screeners and supervisors as necessary, to help certify screening equipment, and to ensure that security was performed correctly under the direct supervision of FAA civil aviation security agents.

The American Association of Airport Executives (AAAE) would act as the clearinghouse for criminal record checks conducted on all persons with access to the secured areas of airports who had not been subjected to previous checks.

FAA Administrator, Jane Garvey, speaking at the Washington National Press Club on October 17, reassured us further: 'Every measure is important and must work together to create a seamless web of security. And, most important, we must stay as committed to this task tomorrow - and into the future - as we are today.'



Some critics have called for Jane Garvey's resignation as head of the FAA

THE ADMINISTRATOR

Jane Garvey is the Administrator of the FAA. For clarity, according to the FAA's own literature 'The FAA is the element of the U.S. government with primary responsibility for the safety of civil aviation'. In light of this unequivocal mandate, one has to question their apparent non-presence. Of course, we caught a glimpse of the Administrator at O'Hare Airport on September 26 but where was she as the FAA's senior executive before that? Of course, the public appreciates that the Department of Transportation has taken the 'public' lead but why is the element of the U.S. government with primary responsibility for the safety of civil aviation so reticent? Why were the majority of the Administrator's public speeches confined to testimony?

One would have thought that the FAA had a unique perspective; after all, their Administrator was a former Director of Boston Logan Airport, the very same airport that two of the planes involved in the September 11 atrocities departed from? Who better to know the 'hands on' reality of security at our airports?

The fact is that the events of September 11 not only redefined our collective concept of terrorism but also brought the FAA under the microscope once more.

THE INACTION

In her statement before the Committee on Commerce, Science and Transportation, Subcommittee on Aviation on the status of Security

Equipment, on November 5, 2001, Jane Garvey stated ‘The assumptions and strategies that were the basis of aviation security, a few short weeks ago are being reassessed’. Is it correct to assert that the events of September 11 spawned a host of security concerns that were not already known? Is it not the case that the measures implemented post September 11 were ones that had already been recommended or otherwise mandated? Did the FAA ‘work tirelessly to identify and implement needed changes’ before September 11?

THE SCREENING COMPANIES

Screening companies have been dubbed a ‘key line of defense against the introduction of dangerous objects into the aviation system’¹ and yet despite their critical role in securing our nation’s airports, efforts to regulate them have been plagued by procrastination and delay.

The White House Commission on Aviation Safety and Security issued an initial report on September 9, 1996, with 20 specific recommendations for improving security, one of which was the development of uniform performance standards for the selection, training, certification, and recertification of screening companies and their employees.

These recommendations were given added impetus by virtue of Section 302 of the Federal Aviation Reauthorization

¹ GAO June 2000 Report “Long-Standing Problems Impair Airport Screeners’ Performance”

Act of 1996 that directed the Administrator of the Federal Aviation Administration to certify companies providing security screening and to improve training and testing of security screeners for providing security screening services.²

In early 1997, the FAA sought public comment on issues relating to FAA certification of screening companies and other enhancements to air carrier screening of passengers, property and baggage.

In June 2000, the General Accounting Office reported³ that the FAA was two years behind schedule in issuing its regulation requiring the certification of screening companies.

However, it was not until January 2000 that a Notice of Proposed Rulemaking⁴ was issued concerning FAA certification for security screening companies.

On October 20, 2000, in U.S. District Court in Philadelphia Argenbright Security Inc was sentenced on charges of making false statements to the FAA concerning the training, testing and background verification of employees. An OIG investigation found that in some cases, convicted felons had been hired as security screeners. Argenbright was placed on three years’ probation and was ordered to pay \$1,550,000 in fines and

² Federal Aviation Reauthorization Act of 1996, Pub. L. 104-264

³ GAO June 2000 Report “Long-Standing Problems Impair Airport Screeners’ Performance”

⁴ Docket No. FAA-1999-6673; Notice No. 00-02; AG84

restitution. On October 11, 2001, the U.S. Attorney's Office for the Eastern District of Pennsylvania filed a petition to order Argenbright to answer charges that it continues to violate the terms of the probation order regarding the hiring of screeners at Philadelphia International Airport without appropriate background checks or training.

On December 12, 2001, we learn that 69 workers at the Salt Lake City Airport were indicted on charges of lying to their employers about their immigration status or criminal background and providing false Social Security numbers on their application for security badges.

So how is the flying public safer since the plethora of reforms promised since the TWA 800 accident? Is it correct to say that 'the TWA 800 accident invigorated and accelerated a process already under way'⁵ that culminated with the creation of the 'Aviation Security Advisory Committee Baseline Working Group'?

THE SCREENERS

The FAA monitors the performance of screeners by periodically testing their ability to detect potentially dangerous objects carried by FAA special agents posing as passengers. In 1978, screeners failed to detect 13 percent of the objects during FAA tests and in 1987, screeners missed 20 percent. Test data for the period 1991-1999 showed that the declining

⁵ FAA NEWS June 2001 "Fact Sheet: Security Actions Taken Since the TWA 800 Accident"

trend in detection rates continues. One would have thought that this would compel the FAA to get tough on screeners' performance. According to a June 2000 report to Congress⁶:

'... during 1999, FAA increased the number of tests using the more easily detected standard objects and decreased the number of tests using the more difficult-to-detect explosive devices. Consequently, FAA showed progress toward achieving its goal when, in fact, no progress had occurred.'



Public confidence in airport security is not helped by the widely reported security lapses since September 11

When one combines this observation with those of Gerald L Dillingham, Director, Physical Infrastructure Issues, on September 20, 2001, that 'More recent results have shown that as testing gets more realistic-that is, as tests more clearly approximate how a terrorist might attempt to penetrate a checkpoint -

⁶ GAO June 2000 Report "Long-Standing Problems Impair Airport Screeners' Performance"

screeners' performance declines significantly,⁷ one is left with a very



Let us all hope that the promises of today are more reliable than the many promises made in the past.

alarming picture of the reality of the FAA's commitment to improving screener performance. The latter also stated that the 'FAA's efforts to address these problems have been slow'. Kenneth M Mead is the Inspector General of the Department of Transportation was even less reticent in his assessment of the FAA's efforts:

'FAA has acknowledged that screeners' detection of dangerous objects during testing is unsatisfactory and needs improvement. This is a long-standing problem – one that we reported on over a decade ago'⁸

It is hoped that the TIP (Threat Image Projection) system will significantly improve screeners' performance and as the Administrator stated on July 19, 2000 the FAA was 'replacing every airport security checkpoint X-ray

machine in the country with X-rays installed with our new threat imaging software.'

TIP is a computer software program, which projects fictitious images on to bags or an entire fictitious bag containing a threat. TIP is intended to keep equipment operators alert, provide real world conditions, and measure performance in identifying the fictitious items or bags. According to FAA spokesperson Paul Takemoto⁹ only 600 TIP units have been installed out of a target total of over 1400; a miserable 42%.

THE LESSON

In 1988 we were assured that security was a priority after the bombing of Pan Am Flight 103. In 1996 we were assured that security was a priority following the crash of TWA Flight 800. In 2001 we are told the same thing. The FAA has singularly failed in its efforts, or lack thereof, in making our nation's airports safer. They have been slow to respond to genuine documented concerns and have failed miserably in bringing about the plethora of reforms that follow an aviation tragedy. For all the action that has characterized post September 11 it is dwarfed by comparison to the years of inaction and procrastination.

Let us all hope that the promises of today are more reliable than the many promises they made in the past.

⁷ "Terrorists Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports" September 20, 2001.

⁸ "Actions Needed to Improve Aviation Safety" September 25, 2001.

⁹ Sourced from "Facing a New Menace" Scientific American September 11, 2001



The Impact of Aviation Security on airline travel. Will it ever be the same?

By

Jim Bennett

Jim Bennett, IASA USA Director of Aircraft Safety & Security, divides his time between the US and Chile. Over the past three months he has extensively promoted IASA's interests in South America You can contact him by email at:

IASA.LATAM@WORLDNET.ATT.NET

The recent air piracy and hijackings of commercial airliners on Sept. 11, 2001 have caused a national emergency requirement to upgrade airport and civil aviation security measures. Those events, for the moment have caused IASA to shift emphasis to report on aviation and airport security. IASA remains committed to reporting on aviation safety related matters and there remains considerable interest to resolving many longstanding aging aircraft, defective wiring problems and other important aviation safety issues.

Like Dec. 7, 1941, the events of Sept. 11, 2001 will be etched into our history as another day of infamy. It is hard for anyone to conceive how four separate airliners could be hijacked by four different teams of terrorists from three different US airports, commandeered as weapons of mass destruction in unprovoked attacks on targets of strategic economic and military importance to the United States.

These hijackers penetrated airport security in each case using commonly available box cutter knives that were not challenged by airport security screeners. The group of 19 hijackers operated in four different teams and had trained for years for this heinous mission as ordinary, law abiding citizens, receiving sufficient air transport pilot training to pilot the planes and then purposely crash them after commandeering them from the pilots in command. The existing philosophy prior to these events towards hijackers never considered a situation where a suicidal pilot would take such

action. It was always our position that the flight crew capitulate to the hijackers to avoid damage to the aircraft and to minimize any risk to passengers. Our airport and aviation security regulations (FAR 107 and FAR 108) enacted since a bomb destroyed Pan Am 103 in 1988 and other air piracy hijackings dating from the 1970s failed to deter these acts.

The Sept. 11 events will forever change commercial air travel, as we knew it. The Aviation Transportation and Security Act of 2001 (Public Law 107-71) became effective on Nov. 19, 2001. The new legislation consists of 132 pages including the final enriched version of Senate Bill S.1447 and the House of Representative's amendment, House Conference Report 107-296.



John Magaw is the new security czar.

This law completely reorganizes aviation security, transferring all aviation security control from the F.A.A. to the Department of Transportation into the new agency called the Transportation Security Administration (TSA). President Bush named former Secret Service chief John Magaw as undersecretary of Transportation for

security. The new law addresses a number of airport and security deficiencies and should resolve many of the deficiencies of the system that have accumulated over the last 12 years.

The following are the main points of the Aviation Transportation and Security Act of 2001:

Section 101 – Transportation Security Administration

Creates a new administration and will be under the management of the Under Secretary of Transportation for Security. He/she will be appointed by the President for a term of 5 years and be responsible for all modes of transportation security including air, rail, sea and highway and will report to the Secretary of Transportation at DOT. All civil aviation security functions currently performed by the FAA must be transferred to the new agency by Feb. 18, 2002.

Section 103 – Federal Security Managers

A new federal security manager will be appointed by the Under Secretary for each US airport to oversee screening and other security duties.

Section 104 – Improved Flight Deck Integrity Measures

Effective immediately, the FAA shall issue an order to prohibit access to the flight deck to unauthorized persons, require the strengthening of cockpit

doors and locks, require that the doors remain locked except to allow ingress and egress by authorized persons, to prohibit any flight crew member except those authorized to the flight deck from having a key to the cockpit door lock; and, to take action as may be necessary including modifications to procedures including flight deck re-design.

Implementation of other methods:

The FAA may develop and implement other methods to employ video surveillance systems to alert pilots in the flight deck of cabin activity, to ensure continuous operation of an aircraft transponder in event of emergency, to revise procedures by which cabin crews can notify flight deck crews of security breaches in the airplane.

Section 105 – Federal Air Marshals

The Under Secretary has the discretion to provide marshals for every flight determined to be “high security risks”.

Section 106 – Improved Airport Perimeter Access Security

Requires immediate screening of all individuals, goods, property, vehicles, etc. before entering an airport secure area. Screening requirements for any person entering the airport secure areas shall offer the same level of protection as that offered for screening of passengers and baggage. The Under Secretary must establish a pilot program consisting of at least 20 airports to evaluate new technologies for access

control systems and other security measures for airport secure areas.

Section 107 – Crew Training

Prior to Jan. 18, 2001, the Under Secretary shall develop detailed guidance for training flight deck and cabin crews to prepare them for potential threat conditions including determination of the threat level, crew communications and coordination, appropriate defensive responses, use of protective devices, psychology of terrorists to cope with their behavior and passenger responses, live situational training exercises, flight deck procedures or aircraft maneuvers to defend the aircraft, and any other subject pertinent to this area. The air carriers have until Mar. 18, 2001 to develop a flight deck and cabin crew-training program and present it to the new Administration then who has 30 days to review the program for approval. The carrier has 180 days after receiving approval of its aircrew-training program to accomplish all required crew training.

Section 108 – Security Screening by Private Companies

A pilot program for up to five airports (Risk categories X, 1, 2, 3, and 4) must be established to conduct security screening through a private company. Those five US airports will apply for entry to the program and the Under Secretary will execute a contract with a private contractor. Each airport will have federal security supervisors to oversee all screening and a federal law enforcement officer assigned to each

participating airport. This program is expected to commence sometime during Dec. 2002 and end in Dec. 2004. Contractual award preference will be directed to companies owned and controlled by a US citizen. Screening companies competing for this contract must have standards as high as the federalized force. After two years, US airports can apply to opt out of the federalized screening force and hire a private contractor under the same guidelines as above.

Section 109 – Enhanced Security Measures

The Under Secretary may require an “effective” 911 emergency call capability for onboard telephones serving passenger airplanes and passenger trains. Also a standard ID system for state and local law enforcement for use in obtaining permission to carry weapons in aircraft cabins and obtaining access to an airport secure area. The Under Secretary may also establish a “trusted passenger program” wherein air carriers may employ available technology to check the backgrounds of passengers who elect to join the program, speeding their passage through the system and allowing security to focus on others not enrolled in the program.

Section 110 – Screening

Physical screening of all passengers and property carried aboard a passenger aircraft, including mail, cargo, carry-on and checked baggage will be conducted on all flights originating in the US will be accomplished by a federal employee

– with the exception of the five designated airports under the pilot screening program. A system to inspect all checked baggage must be in place as soon as possible but no later than Jan. 18, 2002. The Secretary of Transportation shall take all necessary action to ensure that explosive detection systems are deployed as soon as possible to all US airports to screen all checked baggage and that US airports have a sufficient quantity of explosive detection systems to screen all checked baggage no later than Dec. 31, 2002. If explosive detection equipment at an airport is unavailable, all checked baggage must be inspected for explosives using alternative screening means. The alternate screening method may include a bag-matching program that ensures that no bag is placed on an airplane without the person who checked the bag actually boarding the plane (100% matching required), a manual search of the checked baggage (including the consideration of using National Guard troops for the manual search process), bomb sniffing dogs, or other technologies.

An exception to the mandatory explosive detection inspection of checked bags is provided to the baggage of passengers subjected to the Computer Assisted Passenger Pre-Screening System (CAPPS) and to known shippers and with the exception of positive bag-matching programs. (The latter introduces some concern because it is a moot point to match baggage to a passenger in the case of a suicidal terrorist).

The federal screeners and all support personnel such as law enforcement must be in place by Nov. 18, 2002. All screeners will be uniformed personnel working for the Transportation Security Administration, which can dismiss anyone performing the screening. Screeners as federal employees can organize unions but are prohibited from striking. At least one armed law enforcement officer will be in place at each screening location.



While much media attention has focused on passengers, the new Act also makes provision for cargo

A system to inspect the cargo on an all-cargo carrier must be in place “as soon as practicable”. No specific deadline is established.

Section 111 – Training & Employment of Security Screening Personnel

The Under Secretary will establish minimum qualification standards for the federalized screeners including a personnel selection exam, be a US citizen, with a minimum of a high school education, pass a criminal background check and be proficient in reading and speaking English. Screeners are required to complete 40 hours of classroom training, 60 hours of on-the-job training (OJT). Screeners can be members of a

trade union but are prohibited from striking. They are also subject to immediate termination without appeal in the case of negligence or dereliction of inspection duties.

Section 113 – Flight School Security

This section is directed to aliens attempting to obtain flight training in air transport aircraft and requires the prospective student to have been authorized by the Immigration and Naturalization Service and the Attorney General's office for such training.

Section 114 – Increased Penalties for Interfering with Security Personnel

Fines and imprisonment of up to 10 years will be imposed on anyone interfering with or assaulting a federal, airport or airline employee with security duties inside an airport.

Section 116 – Security Service Fee

Air carriers are authorized to charge each passenger a \$2.50 security services fee for each leg of a flight with a maximum of \$5.00 per flight

Section 117 – Passenger Manifests

No later than Jan. 18, 2002, each air carrier operating into the United States shall commence the electronic transfer of passenger and crew manifests of persons aboard any plane intending to land in the US to the US Customs Service. This information shall consist of name, sex, date of birth, country of citizenship; passport and/or visa number

and it shall be transmitted in advance of the arrival of the aircraft in the US.

Section 120 – Chemical and Biological Weapon Detection

The Secretary of Transportation may require airports to maximize the use of equipment designed to detect or neutralize potential chemical and biological weapons.

Section 126 – Less-than Lethal Weaponry for Flight Deck Crews

The National Institute of Justice shall assess the range of less-than lethal weaponry available for use by a flight deck crewmember to temporarily disable incapacitate an individual who poses a clear and dangerous threat to the safety of the aircraft, its passengers, or individuals on the ground. It will report its findings to the Secretary of Transportation no later than Feb. 18, 2002. Based on the results of that report, the Secretary may authorize the deployment of less-than lethal weaponry for use by flight deck crewmembers. (Note: there is no wording in the law to require the aircraft manufacturer to review the potential impact on the integrity of the aircraft control or the

electronics systems in the usage of any such weapon).

Section 127 – Mail and Freight Waivers

The Secretary of Transportation may grant a complete or partial waiver on any restrictions affecting the transport of freight, mail, emergency medical supplies, personnel, or medical patients on airplanes during a national emergency.

Section 128 – Flight Deck Security

The pilot of a passenger aircraft operated by an air carrier in air transportation or intrastate air transportation is authorized to carry a firearm into the cockpit if:

The Secretary of Transportation authorizes the placement of a weapon on the airplane, the air carrier approves it, the Under Secretary of Transportation of Security approves the firearm and, the pilot has received proper training for the use of the firearm, as determined by the Under Secretary.

JB



Third International Aviation Security Technology Symposium

On November 28, 2001, the FAA sponsored the third International Aviation Security Technology Symposium in Atlantic City, New Jersey, which consisted of a four-day gathering of government leaders, vendors and experts. Both Mrs. Lyn Romano, Chairman International Aviation Safety Association (IASA) and Ms. Charlene Frenette, CEO – Canada (IASA) attended the symposium.

Presentations on Technology Integration, Human Factors and Trace Detection were held by representatives from the FAA, as well as an Emerging Technologies session, which was co-presented by Transport Canada, and the FAA. The symposium featured numerous diverse security topics including deployment of new explosives detection equipment, emerging technologies, aircraft hardening initiatives and cargo screening. Those in attendance had the opportunity to view over 40 vendors' security technologies. The Symposium, which was organized prior to September 11, drew in more than twice the amount of participants as it did five years ago, a testament to concern about the security lapses that have occurred recently.

Vendors in attendance demonstrated such products as The BCT 2000, a bottle content tester capable of detecting liquids in bottles that may carry a dangerous substance such as gasoline and flagging nitro-glycerin. The I-Portal 100, a walkthrough Quantum Magnetics metal detector that captures a digital image of a passenger and transfers it to a computer screen, with flashing dots denoting hidden metal. It can reduce the time spent by an airport screener by narrowing the search to one area of the body. The Jet Stream, an iris-recognition system sold by EyeTicket Corp, uses a scan of the eyeball for quick identification of a traveler's identity. Heathrow Airport in London was scheduled to begin using this technology January 2002.

In order to meet the December 31, 2002 goal of 100 percent Early Detection System screening of all checked bags, over 2,000 EDS must be deployed, that amounts to over 1,800 more than are currently available. In a statement made to Symposium participants, FAA Administrator Jane Garvey acknowledged before September 11, civil aviation was the "symbol of commerce" now, it has changed the way national security and aviation security are viewed. Ms. Garvey asked for the assistance and expertise of the security technology community, "We need your commitment". In a statement to the Subcommittee on Aviation, Committee on Transportation and Infrastructure, US House of Representatives on December 7th, 2001, Mr. Frank Vehlen, Executive Vice President and Chief Operating Officer of Heimann Systems Corp stated the following:

- "100% screening of all checked bags by December 2002 is not realistic."
- "Deploying the present certified technology, which is all CT based, is extremely costly both in implementation and in operation."

- Prior to September 11, the goal of the FAA was to start the phasing in of 100% checked baggage screening by 2009 and complete it by 2014. This was a timeframe of 13 years. Now we want to achieve this goal in 13 months?"
- "The FAA in the International Aviation Security Technology Symposium held last week in Atlantic City, stated that between 2,200 and 2,300 CT's would be needed to accomplish 100% inspection of all checked bags in the US. The manufacturer's current capacity- only two companies have a CT product that is FAA certified – does not allow for the manufacturing of over 2 thousand units in one year. Even if they were able to ramp up production, most airports will not be ready to receive the units by the 2002 deadline."
- "Lets look at other aspects related to the deployment of CT's in the lobby of airports. The footprint needed for a CT including space for operators, passengers and queuing, is at least 20' by 30' or 600 sq.ft.per CT. An airport such as O'Hare in Chicago would need over 100CT's. This represents lobby space the equivalent of approximately 1.25 football fields.

Mr. Vehlen stated he believed a multi solution approach would improve security, be operationally practical, will meditate risk and avoid wasteful spending.


The Symposium was not without skeptics, even among the exhibitors who were anxious to acquire FAA monies for their products. Richard Marchi, a senior vice president with Airports Council International-North America, was quoted in the Dallas Morning News as stating that it was a "seemingly impossible schedule," noting that a single X-ray machine can take months to install.



Cathal Flynn, former Security Chief for the FAA told USA Today, he could not understand how 100% checked baggage could be done by the deadline, while Officials at InVision Technologies and L3 Communications, the two firms certified to make the screening machines are making only a handful each month. It will take months to ramp up production, and they say no more than 1,200 machines can be produced by the end of next year, far short of the number required.

In her closing remarks to the Symposium attendees, Ms. Garvey, FAA Administrator stated, "We need to exploit technology. We need to improve security. We need to do it now. And we will."

CF



Like a Curate's Egg, Good in Parts - but salvaged, bogus or unapproved?

By

JOHN SAMPSON

John serves as Director of Aircraft, Engineering & Technical Operations and is CEO of IASA Australasia.

You can contact him by email at: safety@iasa-intl.com

Recently the FBI started a criminal investigation into whether or not the American Airlines Airbus that crashed in Belle Harbor NY had any parts on it that might have been supplied by an Italian operation that was cannibalizing aircraft being taken out of service. PanAviation was supplying the bits and pieces worldwide as the genuine refurbished article - but with bogus paperwork. That investigation turned up nothing in respect of AA Flt 587, but it served to highlight a problem that has festered within aviation maintenance for many years. Because of the high mark-up on bona-fide aircraft parts, there is much incentive for criminal elements to bodgy up reclaimed parts as the genuine article - the profit margins can be huge.

The FAA has a "suspected unapproved parts" division, however it is very much like my old Ford. It needs kick-starting to get it going. Others have likened it to the well-known "Uh Oh Brigade". That's the name given to the group that always gathers around an accident scene and says collectively: "Uh oh, looks like there's been an accident". The bleeding obvious is that there is a sizeable underground trafficking in bodgy parts going on - but because it is so lucrative it might be both dangerous and commercially unproductive to highlight its existence. Let's face it, if an organization like the one in Italy is pulling surplus Airbus to pieces and flogging off those parts, there's likely to be a sizeable market for them. Those appreciative brokers and buyers are not likely to ask where that part came from, whether or not they suspect its provenance. Perhaps we're talking mostly about the Third World here - and perhaps not. Once it's in it's in. If it looks the part and it fits and it comes with some convincing (though counterfeit) paperwork, it's found a home for life. Well OK you might ask,

who's the victim? Some would say it's the bona-fide middleman who misses out on his cut. Others would say it's the manufacturer who reserves the right to "overhaul" said parts and charge outrageously for that "droit de seigneur". Aviation Safety proponents might say that the victims are those who could die when that worn, rejected or non-reconditioned (or perhaps even completely bogus) component forms part of an accident chain. Are there any examples of this having happened? Are there "chop-shops" out there fabricating "made-to-order" (or high turn-over/in-demand) parts? With the number of aircraft now parked in desert bone-yards for break-up disposition, how many graveyard employees are ghoulishly robbing? How many of the myriads of parts-brokers are "involved"?

A Presumption of Innocence

Firstly it must be pointed out that the NTSB (and other national accident investigatory bodies) will be working on a presumption of innocence and not actively looking through wreckage for suspected unapproved parts (SUP). So who's to know how many duff parts have been complicit in failures? Outside airline aviation there have been ample instances of incident aircraft being found to have SUP parts - and they have caused accidents. Within airline aviation there are manifold instances of incorrect parts being fitted and parts being omitted or fitted incorrectly - however the fitment of bogus parts, that seem to "fit the bill", can become easily lost in the amorphous whole. Whilst the FAA has ample established reporting procedures for initiating action on SUPs, it is quite evident that a cunning operator can easily circumvent detection. It was only (as is often the case) because the Italian Connection got sloppy and blatant, that it was detected. The question remains extant - how widespread is the practice? The Business Software Alliance is funded by software corporations with much to lose if counterfeit software was to go unchallenged - so why doesn't Boeing have its equivalent agents in the field? The simple answer is probably that so many firms are involved as suppliers and no-one is solely motivated to "get any acts together". At the end of the day it is the regulator that must run an effective program and not just passively maintain a channel for reporting. So what constitutes an effective and foolproof program for parts identification, one that can be followed up as if it had its own Social Security Number?

Perhaps you could agree that it's time someone:

1. blew the whistle on the evident absence of any such validation methodology. Any scheme that relies upon intrinsic honesty is about as effective as a bank with a walk-in serve-yourself vault. The FAA's specialists are obviously an exercise in tokenism and very thorough paper-tigers.
2. suggested a viable alternative
3. protested strongly that 9/10ths of this iceberg unclearly remains underwater and unobserved.

Post-911 and Enron, the only thing that can be trusted is a system that engenders trust. Without auditably transparent systems in place, anarchy rules..... and it's always someone else's fault.

The IASA Proposition

The software and music industry is now applying non-reproducible holographic labels to CD's so that it's readily apparent when something is not kosher. Most currencies are making the switch to similar technologies (e.g. Australian plastic bank-notes have a holographic transparent window). Australia is now making such notes for a whole host of other countries.

So IASA offers this solution:

- A. First obstacle (provenance). Each yellow label should incorporate a hologram unique to the FAA Certified Repair Station (CRS) allegedly issuing the part as reconditioned.
- B. Each CRS, once it has reconditioned (zero-houred) an item, will need to issue a serial number that gets affixed to the "yellow label" and then heat-shrink package it before shipping. The history of that serial number also gets web-mounted within a database. A Wichita FBO CRS might for instance have an accreditation for repair of transponders. Its serial number might be prefaced WICH12- (and then some four alpha-numeric blocks that identify the part-maker, type-part, date of original manufacture and etc).
- C. Now for the cunning part. Using PGP cryptography, each label would have a magnetic bar code inserted. This would be the public key. Using a magnetic (versus optical) bar-code reader, anyone applying that part must first "read" that public key. This puts the onus upon the user (i.e. where it is now) but makes it impossible to claim that a part was undetectably counterfeit. How so? The reconditioner of the part would have used his "private key" (known only to him) to insert the serial number on the yellow label. That serial number, once turned up via the database, gives the exact same data placed upon the Internet database by the reconditioning CRS. It identifies the "who, when, what and where" relevant only to that unique part.
- D. Whilst that part is on an aircraft, the detached label itself becomes part of the aircraft's maintenance paper work and is in its electronic record.
- E. If a part is applied to an aircraft using this process, yet later found to be bogus or "suspected unapproved", then only the Certifying Officer at the CRS can be the culprit (unless he talks long strings of code in his sleep - thus giving away his private key).

Without such a bulletproof system there will always be crook brokers, facilitating intermediaries, nil responsibility, ATA disinterest and buck-passing - because the profits to be made are so great. With such "batching" of reconditioned parts, even "approved" parts that have been poorly reconditioned (and fail prematurely) will fall readily out of such a database. The FAA must "get with the times" and make with a system (such as described above) that is foolproof and criminal-proof. All that's required is some consensus between the big four aircraft-makers. Their sub-contractors will readily fall over themselves falling into line.

Pros and Cons

There are really two issues here. Bogus parts are those manufactured under "phony" PMA (parts manufacturing authority). PMA is a certificate from the FAA that the parts-maker's parts conform to the original manufacturer's specifications. Phony PMA parts have been found by FAA inspectors here in the US some time ago. Cannibalized parts that are re-sold are very common and legitimate. It is OK to do that - provided that the parts have been inspected and are certificated for installation by an authorized and certified FAA repair station.

Italy's PanAviation fraud is a case of cannibalized parts that were re-sold without proper FAA repair station inspection and falsely certified with "yellow tags". i.e. bogus parts (those manufactured using unacceptable materials and processes and perhaps with labels identifying them as PMA certified) are a different issue to using uncertified parts (cannibalized parts lacking an FAA inspection certificate).

The FAA safety inspectors do have a lot of clout and can shut an outfit down as well as fining it heavily. The scope of their authority varies from region to region but they don't mess around when they find an anomaly. The problem is that there are so many of these used parts brokers and dealers out there that they just don't have the staff to police it. Instead they concentrate their activities at the installer's facilities. It is impossible to know what goes on at overseas reclamation sites. The problem generally manifests itself when the part finds its way into someone's stock inventory. If it doesn't have a "yellow tag" it can't be used. Sure, there are possibilities of someone incorrectly or illegally applying a "yellow tag". It's like counterfeit bills. Unless everyone accepting one has a test device to detect funny money, it gets through the system - but at least a phony dollar-bill will get picked up eventually, unlike a part hidden away in an aircraft's innards. So at present they cannot control this illicit trade 100%. But you have to accept that the major carriers will perform very thorough source inspections before they acquire any such parts. It's the fly-by-night outfits or the ones that operate on shoestring budgets (low fares, minimum spare parts in inventory, marginal repair facilities, etc.) that remain a worry.

Input from the CEO of an airline parts company. ... He is bothered by the events in Italy and has some interesting observations. He thinks the situation is indeed serious and is waiting to see how it plays out. His company was approached by the Italian firm that cannibalized the parts but was suspicious about the authenticity of the parts papers and passed on them. He said that his competitors did buy into it. Although troubled by the inability to authenticate valid FAA inspection certificates (yellow tags) or the paperwork accompanying the parts, he believes strongly that no major airline would buy used parts from any overhauled parts shops until their own quality assurance source inspectors had performed a full quality audit of the shops that supposedly certified the parts. If they measured up to the inspections, those particular shops are placed on a qualified supplier list. They will not deviate from that and just don't operate without qualifying the source to the nth degree. Regarding IASA's proposal, how does one prevent some crook from learning the code and affixing phony info? (he queries). The concerns are that the PGP keys might be

accessible to a fraudulent supplier. If so there would be no guarantee that the test certification was accomplished or that the authentication hadn't been falsified.

His company will only buy parts from sources that the CEO (or his inspectors) have personally witnessed testing and from suppliers with whom there is a long track record of business. In other words, you just can't broker aircraft parts like a commodity, although it's conceded that that has been going on elsewhere. The buyer must know who he is dealing with and the complete trail and history of the overhauled or refurbished part - including the calibration data on the test devices, the source and the standards for calibration of the test equipment, fixtures and tooling. Assuredly though, there are still possibilities for manipulating test records.

And that's where IASA's suggestions come into play. Once all handling of a part is totally accounted for and all required tests are performed, then some unique method of tying that test-data back to the identifying characteristics and the identity of the repair shop will be affixed to the part. It can then be safely assumed (or rather, assured) that the part is in fact a bona-fide authentic and certifiably acceptable part for installation. The question is, who maintains the keys to the store to assure that some bandit doesn't learn the technique and find a way to forge realistic data on a part?

So how does one prevent some crook from learning the code and affixing phony info? The concerns are that the keys might be accessible to a fraudulent supplier and so still no guarantee that the test certification was accomplished or that the authentication hasn't been falsified.

A Verifiable System

IASA is concerned that no such system is in existence for airplane part identification, authentication and verification. Many of the parts that are being replaced "on condition" (or which are "lifer") would be critical for safe operation (which is why they wear or tend to crack/corrode etc). One would think that such a secure foolproof and fraud proof system (to stop sub-standard or just dubious parts being pressed into service) should be "de rigueur". Once they get to the bottom of this PanAviation scandal it might be apparent that the FAA's suspected unapproved parts watchdog (<http://www.faa.gov/avr/sups/index.htm>) was blind and toothless. We shall see - but perhaps they won't, despite FAR145 having been just "final ruled" for August 2001 - after being in rewrite for 30 years. Perhaps the journalists will get their teeth into this one.

Many industries already use crypto verification. Most academics use the Verisign System to validate their emails (so that they cannot be misquoted). See: <http://corporate.verisign.com/news/fact.html> It is similar to the systems used in electronic commerce to stop fraud. But what about "Universal/International Adoption". I guess you might need a really big disaster attributable to a bogus part in order to force the issue on that score. It'd be something ICAO would not want to be involved in - but it is really within their province.

Doubters might be assuming it would be possible for a crook to get a copy of a particular certifying station's private key (note that I said a particular station, since each would have their own key). But consider that their key would be put into a standalone machine (isolated from any network through which it might be hacked)- a machine that only a single trustworthy person would have access to. The odds of a crook being able to get hold of the private key is therefore very slim - he would either have to break in and physically steal the computer with the key (thence cracking that computer's password), or else the station manager would have to be complicit. Also keep in mind that there is absolutely no reason why the key cannot be changed regularly by its holder (most likely weekly, but even daily). This would be remarkably easy to do, since the new public key would be distributed via the FAA's website. So the crook would have to be able to get regular timely access to the key in order for any profitable criminal scheme to succeed.

Also keep in mind that if a supplied part is found to be fraudulent, then it would be exceedingly easy to determine exactly which supplier is fraudulent, and then launch an investigation into that firm. This is so because each station has its own key, and if a part has been certified, and is later found not to be ship-shape (i.e. is not reconditioned or is bogus), then you instantly know who is responsible. But the whole idea is to preclude that situation from happening (the top-down approach versus the present "base of the parts-pyramid upwards" approach - which has been so often discredited).

So if the test certification isn't done, then again - it is very easy to determine who was involved in skimping on that certification, and so arrest and charge them under the regulation. And as for the authentication being falsified? Can't be done. The text on the sticker that is 'signed' cannot be falsified - it has to be checked by computer of course, but as long as it is, the authentication will remain secure unless the rather unlikely case of someone stealing the key actually happens. At no level will a company be able to itself claim to be duped or a "victim".

So for a criminal, there are only two non-feasible approaches to beating the system: getting regular access to the key as it is changed (weekly/daily), and simultaneously having a couple of co-conspirators on the workshop floor certifying the parts when they aren't in fact being checked or reconditioned. In both of these cases, as soon as a single defective part is detected, you know who to point the finger at. Firstly the station chief (he being responsible for the security of the key), and secondly, the workers on the station floor at the time the certificate was generated (a timestamp is easy to add in). Then all you need do is lookup who was working the shop floor at the time the sticker was generated.... and you've got them cold.

The odds are just not good for a criminal operating within such a system. The only reason there's criminal activity in this area at the moment is because there are so many parts on the market, and the labels are easy to forge. Make it impossible to forge them, and suddenly the profits/risk ratio changes dramatically. If an airline maint dept fits a part without a valid label (which label then becomes part of the aircraft's maint records), then they are imperiling their hull insurance and airline operating certificate.

A Poignant Parallel

Phoned up the supplier of our new fireplace because of a maintenance issue with it. He was able to punch in the serial number and tell me everything about it without any input from me. He was able to verify who installed it, when, where and the warranty date. Yet there are many naysayers who don't see a need for change and believe in the present antiquated system's "integrity". Our consulted parts Company CEO believed strongly that "no major airline would buy used parts from any overhauled parts shops until their own quality assurance inspectors had performed a full quality audit of the shops that certified the parts. If they measure up to the inspections, those particular shops are placed on a qualified supplier list." They "will not deviate from that and just don't operate without qualifying the source to the nth degree." Surely, in light of the implicit admission that there is always difficulty marrying up the paperwork with the part, and that a quality audit is always required, it is a wholly reckless system (if one can call it that). Is it not similar to the statement that "the FAA relies on the airlines to follow ADs and do not supervise their compliance as such". As we now know only too well, some airlines will look to save a buck at every available opportunity - how can some airlines sell tickets at such reduced rates unless they are saving or recouping money elsewhere? Alaskan was prospering until the AK261 calamity dropped their maintenance House of Cards.

Verifiable Integrity or a Tradition of Trust?

IASA's proposal for the authenticity labeling of bona-fide a/c parts could provide unbeatable security and systemic integrity. If you've understood the problem, then you just may now be wondering how many airplanes are flying around with dubious parts ("unsuspected unapproved"). Bearing in mind that airline maintenance is already computer intensive and that ACO's already have to sign their life away, it's no greater imposition for them to abide by such a system in order to defeat a fraud that may carry with it a death penalty for the unsuspecting passenger. As for the classically disinterested airline - that would rather not know whether their broker intermediary is sourcing shaky parts from a bone-yard somewhere, the onus would be back upon them to verify authenticity (in lieu of: "But my regular parts broker guaranteed these parts and we've always sourced elevator actuator widgets through him").

When you consider what Valujet and Alaskan were up to with their maintenance "pencil-whipping" exercises, the blood runs cold as you quietly consider how much of this particular ice-berg still lies beneath the surface, sight unseen - and how many fingers might be crossed behind backs.

You need to appreciate the subtle nuances and cunning of PGP - and appreciate the impossibility of beating that system. Think of it as you, yourself trying to claim on your home insurance and the claims manager saying: "But Mrs. Romano, the reason why your home contents insurance is so cheap is that the only way a burglar can access your property without alarming the whole neighborhood is if you gave him your alarm code. You can take us to court but the whole system is based upon your not doing that." That's a reasonable (if rough) analogy designed to demonstrate that

any code-based security system is designedly fraud proof – and that of course, in this case, only you yourself could have been the cat-burglar.

LINKS

Bogus Parts (House Valujet Inquiry)

http://commdocs.house.gov/committees/trans/hpw104-48.000/hpw104-48_0.htm

The FAA's 28 hour SUPS course

<http://www.academy.jccbi.gov/catalog/html/21026.htm>

The Arrow Air Case (1994 - \$3M criminal fine)

<http://www.dot.gov/affairs/1998/oig1198.htm>

Mary Schiavo's Case of Bogus Parts

http://www.iasa-intl.com/folders/Safety_Issues/others/flying3.html

FAA Office of Regulation

<http://www.faa.gov/avr/index.htm>

FAA Suspected Unapproved Parts Program Office

<http://www.faa.gov/avr/sups/index.cfm>

Advisory Circular 21-29B Change 2: Detecting and Reporting Suspected Unapproved Parts

<http://www.faa.gov/avr/sups/change2/ac21-29b.htm>

Bogus Parts in Airliners, Where's the FAA?

<http://www.businessweek.com/1996/24/b34791.htm>

The New FAR Part 145 (U.S. and FAA-certified foreign repair stations)

http://www.iasa-intl.com/folders/Safety_Issues/others/thenewpart145.htm

Aviation Security in Canada

At What Cost?

The Canadian Government recently responded to the security concerns of the nation by creating, through legislation, the formation of the Canadian Air Transport Security Authority, responsible for the provision of several key air security services including the management and delivery of pre-boarding screening at airports. A government commitment of \$2.2 billion for aviation security was announced December 2001, including over \$1 billion over the next five years for the purchase, deployment and operation of advanced explosives detection systems at airports across the country.

The authority will be a federal entity and will report directly to the

Minister of Transport. Although the Authority is responsible for consistency of screening services across the country, this may prove to be a difficult task, as they have the power to either recruit their own security officers, or enter into arrangements with airport authorities, or

***IASA CEO,
Charlene Frenette,
looks at the impact
of the Canadian
Aeronautics Act and
asks whether the
true cost of the
proposals under
review is to lessen
accountability.***

***You can email
Charlene at
[CharlyFrenette@hfx
.eastlink.ca](mailto:CharlyFrenette@hfx.eastlink.ca)***

yet again to enter into service contracts with security organizations in Canada, as the situation deems necessary.

Additional security measures were added for heightened policing at airports, air marshals on "selected" domestic and international flights as well as aircraft

modifications resulting from new standards and regulations currently in development with the FAA.

In a recent response from Transport Canada to an IASA representative's list of aviation security concerns, it was confirmed that not all checked baggage is being screened in Canada. IASA was unable to discover any information regarding what detection equipment is currently in use, as Transport Canada stated "Information on equipment types currently in use is not disclosed for security reasons." IASA inquired as to whether the passenger to baggage check performed at the departure airport, is also performed at intermediate en route airports, or if it was assumed the passenger has indeed boarded on to a connecting flight. The response was again, "The answer to this question would require disclosure of the details of security measures which is prohibited by law."

Currently the Canadian Aeronautics Act is under review. While IASA fully

aviation security and safety procedures, and recognizes, at times, the necessity of privileged information in accomplishing this; the following excerpts from a proposal to amend the Aeronautics Act cause reason for concern.

"The amendments to the Act will provide that the safety data collected, analyzed and/or reported by the operator or service provider will be treated as confidential and may not be communicated to any person without the consent of the operator or service provider. Appropriate amendments will be recommended to the Access to Information Act to prevent disclosure of safety data under that Act."

"The Act will provide that the data may not be used in any legal, disciplinary or other proceedings, unless the public interest in the administration of justice outweighs the public interest in keeping the data confidential."

IASA feels that if these measures are implemented, there will be a lack of accountability on many levels.

In summation, there are few outstanding revelations in the Canadian Government's upgrading of aviation security. However, the Canadian traveling public will notice an extra \$24.00 security charge on a round trip ticket. IASA has not been able to ascertain, exactly where these funds will be used in revamping Canadian aviation security. Screeners in Canada are not government employees as they are in the United States. Canada will remain flexible and allow airports a multitude of avenues to hire private firms, or contract employees as they feel best serves their needs. This raises concerns regarding the continuity of

the screening process across the country. To further demonstrate this, an IASA representative was contacted recently by an Air Canada flight attendant who relayed a significant inconsistency in screening procedures for crew members in a number of Canadian airports.

CF

HAVE YOUR SAY

Would you like us to consider an article for our next edition? Or is there a topic you would like us to cover?

If so, please do not hesitate to contact us. You can email (iasa.pr@virgin.net) or send a fax (+1 775 854 1260) at first instance.

IASA relies on dialogue with others concerned in aviation safety and we hope that you take this opportunity to have your say!



INTERNATIONAL AVIATION SAFETY ASSOCIATION

About Us

On March 4, 1999, Mrs. Lyn S Romano formed the non-profit International Aviation Safety Association (IASA). Lyn's 44-year-old husband, Ray M Romano, was one of the 229 people killed aboard a Swissair operated MD-11 aircraft that crashed off the coast of Nova Scotia, Canada, on September 2, 1998.

Unlike many other aviation safety organizations, IASA is financially and politically independent. IASA does not accept donations and prides itself on its autonomy. IASA does, however, rely on the trust it has built with the many individuals around the world who are able to share their concerns with IASA without fear of compromise.

IASA is committed to ALL aspects of aviation safety, however, our primary concern remains the safety issues associated with aircraft wiring. IASA has been instrumental in raising public awareness of this issue. In May 2000 IASA was praised by the President's Executive Office for bringing these issues to the attention of the White House. Since then IASA has continued to work globally in ensuring that the momentum for change continues unabated.

For more information about IASA please visit our website at www.iasa-intl.com.

Alternatively please email (iasa.pr@virgin.net) or fax (+1 775 854 1260) IASA at first instance.