

JOURNAL OF CIVIL DEFENSE

Volume 37, Issue #3

March 2004

TACDA Officers:

Nancy D. Greene
(President)

Sharon B. Packer
(Vice-President)

Kathy Eiland
(Executive Director)

Regina Frampton
(Secretary/Treasurer)

Board of Directors:

Nancy D. Greene
Sharon B. Packer
Kathy Eiland
Regina Frampton
Dr. Gerald L. Looney
Frank L. Williams
Kevin G. Briggs
Bronius Cikotas
Dr. Art Robinson

Editors:

Alex Coleman
Regina Frampton
Kathy Eiland

Inside This Issue:

U.S. Flights Can Still Be Hijacked, by Aaron Klein

Homeland Security Issues
Transit Alert, by Leslie Miller

Pen Guns – A New Weapon
for Terrorists

NWS Implementing New
NOAA Weather Radio
Warning Event Codes on
June 30, 2004

U.S. Flights Can Still Be Hijacked!

by Aaron Klein, March 03, 2004

[Editor's Note: The following article provides some disturbing insight into the possibilities of additional terrorist attacks on American soil, through what seems to be a widely overlooked or ignored channel, yet one that is ready for the taking, or so it appears. Be advised that this article does outline some very specific ways in which a terrorist possibly could compromise the integrity of airport security by exploiting the known vulnerabilities that exist in the cargo loading facilities of several well-known airports. This article should encourage each and every one of us to make an extra effort to keep our eyes opened at all times for any type of suspicious behavior, as well as to raise our voices to government and private airport security industry to get on the ball and to tighten up the loose ends that still remain in airport security.]

I recently conducted a detailed investigation of security at our nation's airports, and was shocked by the magnitude of deficiencies ripe for terrorist exploitation that I found after visiting various sites and interviewing assorted industry employees from four major airlines. I was disturbed to learn of several easy ways to get any handheld weapon onboard or to place a bomb on almost any domestic flight. It looks like Osama is still in business – U.S. flights are his for the taking.

It seems that most of the post-Sept. 11 security upgrades have been primarily focused on things travelers can see, specifically on increased screening of passengers before they board the plane – including integrated intelligence programs to check passenger lists against databases of possible terror suspects, updated X-Ray and metal-detector equipment at gates, more qualified officials at security posts, and more frequent body searches of passengers before they enter the gates.

But behind the scenes, it's been business as usual. In most airports, aside from more thorough background checks, there has been little or no security measures added to the routines of the tens of thousands of aircraft cargo workers. At many airports, and at most airlines at Miami International, where my research focused, these employees still don't go through metal detectors or X-ray machines, have little direct onsite supervision or outdoor surveillance and, incredibly, in many cases they have separate, unsecured access to passenger gates.

The American Civil Defense Association (TACDA)
P.O. Box 1057, 118 Court Street, Starke, Florida 32091
Toll-free (800) 425-5397 or Direct (904) 964-5397
Online at www.tacda.org

[The Journal of Civil Defense is the official monthly newsletter of The American Civil Defense Association.]

(cont'd)

After the cargo is received in the cargo facility, where maybe 5 percent of the boxes are actually X-rayed or manually inspected, we then have unfettered access to move, tamper, re-label, or add to any shipments. I can put what I want into any container. Plus, I don't go through any metal detectors and I have access to passenger parts of the airport.

To outline a few of my findings, here are some easy, obvious ways to get a weapon onboard at Miami International:

Step 1: Any cargo worker brings a weapon of choice to work in a backpack or on his body, and parks his car in the designated parking area for employees, which is either inside or very close to the cargo facility. The cargo worker enters the cargo building without inspection or having to pass any metal detectors. He then drives his cargo tractor from the cargo building into the Aircraft Operating Area, where he swipes his security card through a magnetic reader and gains access to the "secured" aircraft area, again without ever being subject to metal detectors or inspection. There is a security officer at the AOA entrance who verifies it is, in fact, the employee who is checking in.

Step 2: The cargo guy, weapon in tow, takes any of the ramp-to-concourse elevators by simply swiping his identification badge outside the elevator to open its door and then again inside the elevator to press the second-floor button, again without ever having to pass security or inspection. Cargo man and weapon are now in the concourse, where passengers have already passed through security and have been approved for boarding.

Most cargo workers aren't allowed in the passenger boarding areas, but workers say this rule is not strictly enforced since some cargo employees have business there, such as to coordinate special baggage needs with gate agents or flight personnel. Unauthorized cargo employees routinely enter the gates unchallenged to use the airport restaurants and

stores or to meet family and friends who are flying.

There is even a cargo worker at Miami's American Airlines who brings a bag to work that may include a steak knife for lunch (which usually consists of cooked red meat for their high-protein diet). Once, without consequence, the worker brought the bag onto the employee elevator and into the passenger boarding area, forgetting it contained the knife. The worker claims one can easily pack a gun without anyone knowing.

Step 3: A passenger meets the cargo worker in the bathroom where he passes on the weapon. Now the passenger is armed and ready to hijack.

It's that simple.

And getting a bomb onboard? Any cargo worker can smuggle a small explosive into the AOA using the same method I described above. Keep in mind that once the cargo leaves the cargo building on the worker's tractor, it has already passed any inspection and X-ray. There are many ways to get the explosive on board. Here are just a few:

1) Cargo worker discreetly places the bomb into a Unit Load Device or house container. Cargo workers report that many ULDs are in poor condition with curtains that don't close all the way or doors that don't secure. They can slip the bomb in at any point in their journey from the cargo warehouse to the aircraft operating area.

2) Workers report that many shipments can be found sitting unsupervised at the departure gate several hours before an aircraft's departure. Anyone with access can just put the bomb into one of these shipments, which workers say are rarely subject to secondary inspection.

3) Cargo workers routinely carry small shipments (called hand-carry shipments)

themselves. These shipments are low in weight and would not be placed into the ULDs for space efficiency purposes. Instead, they are randomly tossed by line crew members into the forward, middle or rear cargo hold – inside the plane – without any scrutiny. A cargo worker can just place the bomb into one of these small shipments and carry it to the loading area.

4) Cargo man packs the explosive into one of the many crates or cardboard skids of food the airlines routinely transport. These crates/skids are often damaged during handling, and are open enough to pack the explosive.

5) Cargo workers can go so far as to even bring their own box from home containing the bomb. Cargo workers say that shipment labels can be easily stolen from the cargo facility and used to label the box for the appropriate destination, or a label can be taken from another bulk shipment set for that destination, making it look real. A cargo worker can just bring the box with him on the tractor and put it with the other approved shipments he is driving to the loading area. They say no one would think twice.

If the cargo worker arrives at the departure gate with his homemade box and bomb a bit early, even better. He can just put the box inside the aircraft himself, which would not be uncommon. When the line crew members – whose job it is to actually load the cargo on the aircraft – arrive and see that the shipment is properly labeled, I am told it would be pushed to the rear of the cargo hold without being checked and sent on its way, as does often occur.

There is a crew chief responsible for logging all cargo items onboard the aircraft. He carries a "load plan," which lists weights of every object being stored, and has the exact positions for their loading, which is predetermined by a satellite office. The crew chief conducts a final lockout of the aircraft, which becomes the offload sheet for the arrival city.

But this means nothing. It is not uncommon for shipments to be loaded and dispatched without the crew chief's knowledge. One American Airlines cargo worker told me "things happen so fast, boxes that are not catalogued or part of the crew chief's official manifest are loaded all the time. It's routine. And the crew chief couldn't care less. So it's not a problem."

6) Anyone can just ship the bomb as part of normal passenger cargo /luggage and just take a chance that it won't be inspected. Even though the Transportation Security Administration's deadline for implementing strict government screening of passenger cargo recently passed, most airlines, including many at Miami International, were allowed to revert to private screening companies that many workers say are ineffectual.

A senior crew chief for American Airlines told me that right before the deadline, the TSA brought sophisticated inspection equipment to selected cargo warehouses where the threat was greatest.

"This elaborate show of government technology," he said, "lasted about two weeks. Then the TSA packed up and left the whole inspection process to a private security firm staffed by very poorly trained, low-paid individuals working with antiquated X-ray machines. The machine in my facility has to be at least 30 years old."

"These workers randomly inspect red-flagged cargo having none of the capabilities of the TSA equipment. The machines we are using now depend entirely on the visual skills of the operators, who I catch slacking off all the time."

It's been three years since Osama bin Laden's warriors hijacked our airliners to pull off the most spectacular and devastating terror attack on U.S. soil, and aviation security officials still don't have their acts together.

All of this was partly highlighted Monday, Feb. 23, when 14 airline employees – 11 of them cargo workers – were arrested at Miami International for coordinating the transport of cocaine and heroine from Latin America to other U.S. destinations. The accused allegedly used some of the same methods I described to load over 200 pounds of drugs onto planes and send them to undercover cargo agents in Baltimore, Dallas and Nashville. The cargo workers had been getting away with the scheme for over four years, which implies a major lack of supervision.

I was told by many workers that the government and the airlines are well aware of the enormous security lapses in the cargo department, but that neither is willing to spend the kind of money needed to correct the situation. (Although all government and airline security officials told about the specific lapses

that allow cargo workers to bring a weapon to a passenger claimed to be shocked.)

It's only a matter of time before these lapses are used to hijack or blow up more U.S. airliners, and the governments' and airlines' gross security negligence will be to blame. I strongly suggest they act now.

I've detailed only a few of the many security deficiencies ready for terrorist exploitation that I found. If anyone needs further information, just visit some cargo workers at an airport near you.

[Aaron Klein has previously conducted interviews with Yasser Arafat, Benjamin Netanyahu, Ehud Barak, Shlomo Ben Ami and leaders of the Taliban.]

[The opinions expressed in this article are those of the author(s) and do not necessarily reflect the points of view held by TACDA or any of its officers.]

Focus on Emergency Management and Public Safety

Homeland Security Issues Transit Alert *By Leslie Miller*

WASHINGTON - Homeland Security officials issued a bulletin advising state officials, police and transit and rail agencies to be vigilant in light of the bombings in Spain.

They were asked late Thursday night to consider additional surveillance and to look out for unattended bags and backpacks, Homeland Security spokesman Brian Roehrkas said.

Homeland Security officials were keeping close watch on developments related to the terrorist attacks that killed or wounded about 1,400 train riders in Spain.

Based on the current assessment of intelligence "we have no specific indications that terrorists are considering such attacks on the United

States in the near term," Roehrkas said Friday.

The attacks on Thursday have not prompted the United States to raise its terror alert level, which remains at yellow, indicating an "elevated" threat.

White House spokesman Scott McClellan said the Homeland Security Department has been working with transit officials on emergency preparedness plans.

"Our efforts have focused on awareness, prevention, response, and recovery to a potential attack," he said.

Amtrak increased patrols of its police force and canine units, spokesman Dan Stessel said. Electronic surveillance of bridges and tunnels was intensified, he said. And the company

reinforced its message to Amtrak employees to report suspicious activities to police.

"That gives you another 20,000 sets of eyes," Stessel said. The railroad is continuing to review information received from the FBI and the Transportation Security Administration, he said, but there has been no credible threat against Amtrak or other railroads.

Acting TSA chief David Stone said the agency has been working with public transit systems to close security gaps.

"TSA is very much involved in all risk mitigation plans with trains, metropolitan transit systems and ports," he said.

In New York, Mayor Michael Bloomberg said authorities had moved to increase security in city subways and commuter trains. Uniformed personnel will be present at subway stations and trains, on the Long Island Rail Road, PATH and Metro-North Rail Road trains. Bomb sniffing dogs will also be in use around the region.

"We clearly are focusing, as you would expect us to do, even more resources on the New York City subway system," Bloomberg said at a news conference. "It goes to show we still live in a very dangerous world."

Bruce Hoffman, a terrorism expert at the Rand Corp., said it's much harder to secure transit systems than airports because it isn't possible to closely scrutinize every person in such large crowds.

"If terrorists want to kill a lot of people, public transportation is always the preferred target, because you get a lot of people in the same place at the same time," he said.

Though airplanes continue to be an attractive target for terrorists, he said, the U.S. government's tightening of airport security may have made public transit more vulnerable.

"You harden one target and you shift the threat to another," Hoffman said.

Further, he said, the success of the attacks on trains in Madrid may inspire other terrorists to imitate them.

If the TSA gets wind of a threat, the agency's communication system allows it to communicate quickly with transit agencies, railroads, bus companies and cruise lines, officials said. The agency has given \$115 million in security grants to transit systems in the past year.

James Carafano, a homeland security expert with the conservative think tank Heritage Foundation, said Al-Qaeda has shown an interest in bridges and tunnels. Major subway systems are now closely monitoring tunnels, he said.

"The major subway systems are better prepared than they were several years ago, and that's encouraging," Carafano said.

The Federal Transit Administration has sent technical teams to transit systems to assess their vulnerability and given them grants for training their employees.

In Washington, metro subway platforms were cleared of fixtures that officials thought could be hiding places for bombs. Officials removed trash cans, newspaper recycling bins and newspaper sales boxes.

Mailboxes disappeared from downtown Washington streets as the city tightened its guard against terrorism.

Last month, Homeland Security officials met with a Russian delegation for a debriefing on the February explosion on the Moscow metro that killed 41, TSA spokesman Mark Hatfield said.

"You can bet we're going to be talking to our allies in Spain and try to boil down lessons

learned as the investigation into this horrible attack take place," he said.

[Editor's Note: Since the time this article was originally published, it appears that the number of U.S. allies in Spain, referenced in the previous paragraph has rapidly diminished as a direct result of the newly elected Prime Minister who appears to be significantly less

supportive of the United States' war on terror than was his predecessor. Now we have to wonder how much cooperation we will actually be able to receive concerning lessons learned from the Madrid bombings.]

[The opinions expressed in this article are those of the author(s) and do not necessarily reflect the points of view held by TACDA or any of its officers.]

The Safety Zone

Pen Guns - A New Weapon for Terrorists

[Editor's Note: In the last issue of the Journal of Civil Defense, we began highlighting disguised and unusual weapons that may be used by terrorists to help them gain control in a variety of situations. The cell phone gun, as one example, was introduced as being one of the latest threats to airport security. As addressed in the featured article in this issue, we can see just how easy it might be for a terrorist to hijack or smuggle a bomb on board a commercial aircraft by exploiting weaknesses in the cargo loading infrastructure. With this in mind, let us now consider how much easier it may be for them to carry weapons, that do not look like weapons at all, onto a flight and use them to gain control and create panic. Imagine if you will, for example, a would-be terrorist being able to take control of a commercial jetliner with nothing more than what appears to be an ordinary fountain pen. Consider the following article:]

WASHINGTON - The FBI is warning that terrorists could potentially use pens filled with cartridges of poison as weapons, according to an FBI bulletin obtained by Fox News.

A pen gun is a small-caliber, single shot weapon that resembles a fountain pen.

In its weekly bulletin to law enforcement agencies throughout the country, the FBI said

that bullet cavities of pen guns could be filled with poisonous chemicals or biological toxins, including cyanide, mercury, arsenic and ricin.

"The FBI possesses no information indicating that chemical pen guns are currently being used or will be used in terrorist operations in the United States; however, law enforcement agencies should remain alert to the potential use of such devices," the FBI said in the notice. The FBI noted, by way of background, that Indian authorities in December 2003 seized a pen gun during a raid on a suspected Islamic separatist's home in Kashmir, India. Police also found 25 suspected chemical cartridges. An officer became lightheaded after breaking open a cartridge. However, the chemical agent, if any, has not been identified.

"Pen guns are not new weapons; however, if the cartridges found in the Indian seizure were contaminated, that would indicate a new method of operation," the FBI said.

Since early 2001, several incidents involving pen guns have been reported overseas, according to the FBI. To describe a few:

- On June 18, 2003, Saudi Arabian border guards seized 10 pen guns from Yemeni nationals.

- In January 2003, French police searching locations used by an arrested French Algerian baggage handler found a number of pen

guns. The bureau points out that pen guns can be easily concealed to evade detection at security checkpoints. "Except for its heavier weight, which is evident only when held, a pen gun closely resembles a standard fountain pen. There are no outward markings to indicate the pen is a firearm," the FBI said.

"Furthermore, one type of pen gun has a tiny ink reservoir within the tip, so it will write if the operative is challenged. In a standard X-ray device, an unloaded pen gun may appear as a normal pen."

The FBI said a watch placed on top of a pen gun could obstruct the weapon when going through an X-ray. "Therefore, pens should be separated from other items in screening bins to ensure a clear X-ray image," the agency stated.

Pen guns are readily available in the United States and have recently become available in Europe, the Balkans, Middle East and South Asia, the FBI said.

Fox News' Anna Stolley contributed to this report.

Source: www.foxnews.com/story/0,2933,113259,00.html

[Editor's Note: As you can see, it is more important now, more than ever before, that we all be aware of our surroundings and that we keep a close eye out for suspicious behavior that may potentially prove to be another disaster waiting to happen. Stay alert and vigilant.]

Announcement: Disguised and Unusual Weapons Seminar

The Disguised/Unusual Weapons seminar is four hours of multimedia display and discussion of disguised, unusual and improvised weapons. The design and appearance of these types of unconventional, improvised, exotic, and disguised weapons are only limited by the imagination and capacity of the maker. A fringe benefit of this seminar is the ability to recognize the danger posed by an item before it is used upon you! Introductory cost is \$75.00, which includes manual and certificate.

(Currently this seminar is restricted to Security, EMS and Law Enforcement personnel, only.)

For additional information, please visit www.aiepdisguised.bravehost.com/index.html.

[The opinions expressed in this article are those of the author(s) and do not necessarily reflect the points of view held by TACDA or any of its officers.]

Civil Defense News

NWS Implementing New NOAA Weather Radio Warning Event Codes on June 30, 2004

Beginning June 30, 2004, NOAA Weather Radio (NWR) Specific Area Message Encoding/Emergency Alert System (SAME/EAS) event warning codes will be available nationally for a variety of non-weather events.

The new codes will allow NWR users to program desired alert messages on subjects ranging from child abduction emergencies, local area emergencies, fire warnings, and hazardous material warnings, to radiological or nuclear power plant warnings, shelter-in-place warnings, or volcano warnings.

The NWS is currently upgrading existing warning-generation software and weather radio formatters to handle the new codes. The NWS Office of Climate, Water, and Weather Services (OCWWS) issued a Service

Change Notice regarding the Received: from INTDom-MTA by dohc2.healopic on March 5, 2004.

NWR is the primary means for NWS alerts to activate the Emergency Alert System. EAS event codes are equivalent to SAME codes used by SAME-capable NWR receivers to allow listeners to program desired alert messages. Local or state civil authorities prepare the non-weather related EAS messages, which may be relayed by the NWS over NOAA Weather Radio and the EAS at the request of the message issuer. The NWS does not initiate non-weather related EAS messages.

The event code changes were dictated by the Federal Communications Commission (FCC), which makes the rules concerning EAS, in a Report and Order amending the EAS rules on February 26, 2002. The NWS waited to implement the new EAS event and SAME codes and marine location codes primarily to allow EAS equipment manufacturers time to upgrade their products to accommodate the new codes, and to allow broadcasters time to upgrade their EAS equipment, according to Herb White, NWS Headquarters Dissemination Services Manager, OCWWS.

If new event codes cannot be added to existing NWR receivers, the codes may be displayed as unknown warning or similar message when they are transmitted over NOAA Weather Radio. White said owners of such non-upgradeable radios who wish to receive the new codes would have to purchase a newer model radio receiver.

Owners should check the documentation that came with their receiver, or contact the manufacturer (via telephone or Internet) to see if the new event codes are already programmed

into the receiver, or if they can be added in manually.

The Consumer Electronics Association, an industry group representing designers, developers, and manufacturers of consumer electronics equipment, recently developed a new voluntary standard, which defines minimum performance criteria for consumer electronics products designed to receive digital alert signals broadcast by NOAA Weather Radio and Environment Canada's Weatheradio® Network. The performance criteria include the ability to receive and properly decode all the new EAS event codes.

A range of compliant products will soon be available to the American public. Consumers looking to either upgrade their current NOAA Weather Radio receiver or to purchase a new one should look for them later this spring. Look for the Consumer Electronics Association's new Public Alert designation that will appear on devices carrying public safety alerts broadcast over the all-hazard NOAA Weather Radio system and the Environment Canada Weatheradio® Network.

We recommend customers program their desired new SAME/EAS event codes before June 30, 2004, so the change will be transparent on the effective date, White said.

A complete list of the current and new EAS/SAME codes to be implemented on June 30, 2004, is available online at http://www.nws.noaa.gov/os/eas_codes.htm.

Additional information on the emergency alert system is also available online at http://www.nws.noaa.gov/os/nws_eas.htm and <http://www.fcc.gov/eb/eas/>.

[The opinions expressed in this article are those of the author(s) and do not necessarily reflect points of view held by TACDA or any of its officers.]